



SANGFOR

SANGFOR Technologies Co., Ltd.

International Service Centre: +60 12711 7129 (7511)

Malaysia: 1700817071

Email: tech.support@sangfor.com.hk

RMA: rma@sangfor.com.hk

NGAF V6.4 User Manual



SANGFOR

December 2015

Declaration

Copyright © SANGFOR Technologies Co., Ltd. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Co., Ltd.

SANGFOR is the trademark of SANGFOR Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Co., Ltd.

Table of Content

Declaration.....	ii
Table of Content	iii
Chapter 1 About This Document	xiii
Organization	xiii
Conventions	xiii
GUI Conventions	xiii
Symbol Conventions.....	xiv
Technical Support	xiv
Acknowledgement	xiv
Installation Guide.....	xv
1.1. Environment Specifications	xv
1.2. Power Supply.....	xv
1.3. Appearance	xv
1.4. Configuration and Management	xvi
1.5. Equipment Connection	xvi
Chapter 2 Introduction to the Console.....	1
2.1. Logging In to the Web UI	1
2.2. Configuring and Using the Console.....	2
Chapter 3 Function Description.....	3
3.1. Status.....	3
3.1.1. System Status	3
3.1.1.1 Selecting Panels	3
3.1.1.2 Showing Default Panels	3
3.1.1.3 Viewing Status	4
3.1.2. Security Status	8
3.1.2.1 Events	8
3.1.2.2 Bots	8
3.1.2.3 Data Leak	9

3.1.2.4 Backlink Injections	9
3.1.2.5 Outgoing DoS Attacks	10
3.1.3. RT Vulnerabilities Analysis	11
3.1.3.1 Viewing RT Vulnerabilities Analysis	11
3.1.4. Security Events	12
3.1.4.1 Recent Security Events	12
3.1.4.2 Server Security	13
3.1.4.3 Endpoint Security	13
3.1.4.4 Recent Attack Sources	13
3.1.5. Traffic Ranking	14
3.1.5.1 Top Users by Traffic	14
3.1.5.2 Top Applications by Traffic	15
3.1.5.3 Top Hosts by Traffic	16
3.1.6. Abnormal Connection	18
3.1.7. Flow Control	19
3.1.7.1 WAN Speed.....	19
3.1.7.2 Bandwidth Channel.....	19
3.1.7.3 Exclusion Rule.....	20
3.1.8. DHCP.....	20
3.1.9. Online Users	20
3.1.9.1 Viewing Online Users	20
3.1.9.2 Filtering Online Users.....	21
3.1.9.3 Locking Online Users	21
3.1.9.4 Unlocking Online Users.....	22
3.1.9.5 Forcibly Logging Out Online Users.....	22
3.1.10. Affiliated Source Lockout.....	23
3.2. Network	23
3.2.1. Interfaces.....	23
3.2.1.1 Physical Interface.....	24
3.2.1.2 Sub-Interface.....	26
3.2.1.3 VLAN Interface	27
3.2.1.4 Aggregate Interface.....	28
3.2.1.5 Zone	30

3.2.1.6 Link State Propagation.....	31
3.2.2. Routing	33
3.2.2.1 Static Route.....	33
3.2.2.2 Policy-Based Routing	35
3.2.2.3 OSPF.....	35
3.2.2.4 RIP	42
3.2.2.5 All Routes	46
3.2.3. Virtual Wire.....	46
3.2.4. Advanced Options.....	47
3.2.4.1 ARP	47
3.2.4.2 DNS	49
3.2.4.3 DHCP.....	49
3.2.4.4 SNMP	51
3.2.5. Optical Bypass Module.....	53
3.3. Security Databases.....	54
3.3.1. Vulnerability Database.....	54
3.3.2. WAF Signature Database	55
3.3.3. Vulnerability Analysis Rules.....	57
3.3.4. Data Leak Protection	59
3.3.4.1 Predefined Sensitive Keyword.....	59
3.3.4.2 Custom Sensitive Keywords	60
3.3.5. Malware Signature Database	61
3.3.6. Custom Rules.....	63
3.3.6.1 Custom WAF Signature	63
3.3.6.2 Custom IPS Rule.....	64
3.4. VPN	65
3.4.1. SSLVPN.....	65
3.4.1.1 Online Users	65
3.4.1.2 Deployment.....	66
3.4.1.3 Users	67
3.4.1.4 Resources	80
3.4.1.5 Roles	83
3.4.1.6 Login Options	86

3.4.1.7 Logging In.....	88
3.4.1.8 Authentication.....	88
3.4.1.9 Certificate.....	92
3.4.2. IPSecVPN	93
3.4.2.1 Status.....	94
3.4.2.2 Basic Settings.....	95
3.4.2.3 Local Users	97
3.4.2.4 VPN Connection	107
3.4.2.5 Virtual IP Pool.....	109
3.4.2.5.1. Case Study	111
3.4.2.6 VPN WAN Interface	113
3.4.2.7 VPN LAN Interface	114
3.4.2.8 Multiline Policy	115
3.4.2.9 Local Subnet	116
3.4.2.10 Tunnel Route.....	117
3.4.2.10.1. Case Study	117
3.4.2.11 IPSec VPN	119
3.4.2.11.1. Phase I.....	119
3.4.2.11.2. Phase II	121
3.4.2.11.3. Security Options.....	123
3.4.3. Objects	124
3.4.3.1 Schedule.....	124
3.4.3.2 Algorithms	125
3.4.4. Advanced	126
3.4.4.1 LAN Service	126
3.4.4.2 Multicast Service	129
3.4.4.3 LDAP Server.....	130
3.4.4.4 RADIUS Server	131
3.4.4.5 Dynamic Routing.....	131
3.4.4.6 Certificate Generation.....	132
3.5. Objects	133
3.5.1. ISP.....	133
3.5.2. Application Ident DB	134

3.5.2.1 Viewing Application Identification Rules	134
3.5.2.2 Enabling/Disabling Application Identification Rules	135
3.5.3. Intelligent Ident DB	137
3.5.3.1 Enabling/Disabling Intelligent Identification Rules.....	137
3.5.3.2 Editing P2P Behavior Identification Rules	138
3.5.4. App Ident Rules	139
3.5.4.1 Adding Custom Application Rules.....	140
3.5.4.2 Enabling/Disabling/Deleting Custom Application Rules.....	142
3.5.4.3 Importing/Exporting Custom Application Rules	142
3.5.5. URL Database	142
3.5.5.1 URL Database	142
3.5.6. Services.....	145
3.5.6.1 Predefined Services.....	145
3.5.6.2 Custom Services	146
3.5.6.3 Service Groups.....	147
3.5.7. IP Group.....	148
3.5.8. LAN Server.....	149
3.5.9. Schedule.....	150
3.5.9.1 One-Time Schedule.....	151
3.5.9.2 Recurring Schedule.....	151
3.5.10. File Type Group	153
3.5.11. Trusted CA.....	155
3.6. Decryption	156
3.6.1. Decryption	156
3.6.2. Server Certificate	157
3.7. Authentication.....	159
3.7.1. Local Users	159
3.7.1.1 Overview.....	159
3.7.1.2 Principle.....	159
3.7.1.3 Users	160
3.7.1.4 Deleting Users/Groups.....	175
3.7.1.5 User Import.....	180
3.7.1.6 LDAP Automatic Synchronization	185

3.7.2. User Authentication	197
3.7.2.1 Authentication Policies	197
3.7.2.2 Authentication Options	213
3.7.2.3 External Authentication Server	240
3.7.2.4 Deleting an External Authentication Server.....	243
3.8. Firewall.....	243
3.8.1. NAT.....	243
3.8.1.1 Source NAT.....	244
3.8.1.2 Destination NAT	249
3.8.1.3 Bidirectional NAT	253
3.8.1.4 DNS-Mapping.....	259
3.8.2. Concurrent Connections Control	261
3.8.2.1 Concurrent Connections Control Configuration Example	261
3.8.3. DoS/DDoS Protection.....	263
3.8.3.1 Internet Protection.....	263
3.8.3.2 Intranet Protection.....	269
3.8.4. ARP Spoofing Protection.....	271
3.9. Access Control.....	271
3.9.1. Application Control Policy	271
3.9.2. Anti-Virus Policy	273
3.9.3. APT Detection.....	276
3.9.4. Web Filter.....	279
3.9.4.1 URL Filter	279
3.9.4.2 File Filter.....	281
3.10. IPS	282
3.11. Server Security.....	286
3.11.1. Web Application Protection	286
3.11.2. Server Access Verification	301
3.12. Scanners.....	303
3.12.1. Risk Assessment	303
3.12.2. Web Scanner	307
3.12.3. RT Vulnerability Scanner.....	312
3.12.4. Threat Alerts	314

Traffic Management.....	317
3.12.5. Overview.....	317
3.12.6. Traffic Channel Mapping and Priority	317
3.12.7. Channel Configuration.....	317
3.12.7.1 Traffic Guarantee Channel.....	317
3.12.7.2 Traffic Restriction Channel.....	326
3.12.7.3 Exclusion Rule.....	332
3.12.8. BM Lines	334
3.12.8.1 BM Line List.....	334
3.12.8.2 BM Line Policy.....	335
3.13. System	336
3.13.1. System Configuration	336
3.13.1.1 System Time	336
3.13.1.2 Network Configuration	337
3.13.1.3 Console Configuration.....	339
3.13.1.4 License.....	340
3.13.2. Administrator Accounts	341
3.13.3. High Availability.....	342
3.13.4. Logging Options	346
3.13.4.1 Internal Report Center.....	347
3.13.4.2 Syslog Settings.....	348
3.13.5. SMTP Server.....	348
3.13.6. Email Alarm.....	349
3.13.7. Globally Excluded Address.....	350
3.13.8. Custom Webpage	351
3.13.9. Central Management.....	352
3.14. System Maintenance	354
3.14.1. Update.....	354
3.14.2. Backup/Restore.....	356
3.14.3. Logs	357
3.14.4. Web Console	358
3.14.5. Packet Drop/Bypass.....	359
3.14.6. Remote Tech Support.....	361

3.14.7. Restart.....	361
3.15. Configuration.....	361
3.15.1. Device as a Gateway (Routing Mode).....	361
3.15.2. Data Mirroring (Bypass Mode).....	362
3.15.3. No Change to Existing Network (Bridge Transparent Mode).....	363
3.15.4. User Authentication	363
3.15.5. Server Protection.....	364
3.15.6. Internet Access Protection.....	364
3.15.7. Bandwidth Management	365
3.15.8. Set Attack Reminder and Keep Track of Attacker	366
Chapter 4 Data Center	367
4.1. Statistics	367
4.1.1. Server Security.....	368
4.1.1.1 Example	369
4.1.2. Endpoint Security	371
4.1.2.1 Example	371
4.1.3. Traffic Statistics	373
4.1.3.1 Example	373
4.1.4. Application Statistics	375
4.1.4.1 Example	376
4.1.5. Website Browsing	378
4.1.5.1 Example	378
4.1.6. Antivirus Statistics	380
4.1.6.1 Example	380
4.2. Logs	382
4.2.1. DoS Attack.....	382
4.2.1.1 Example	383
4.2.2. Web Application Protection	384
4.2.2.1 Example	385
4.2.3. IPS.....	387
4.2.3.1 Example	388
4.2.4. Anti-virus	389
4.2.4.1 Example	390

4.2.5. APT Detection.....	391
4.2.5.1 Example	391
4.2.6. Website Browsing	394
4.2.6.1 Example	394
4.2.7. Application Control.....	395
4.2.7.1 Example	396
4.2.8. Local Security Event.....	396
4.2.8.1 Example	397
4.2.9. User Login/Logout.....	398
4.2.9.1 Example	398
4.2.10. Admin Operation.....	399
4.2.10.1 Example	399
4.3. Statistics Report	400
4.3.1. Reports	400
4.3.2. Custom Report	401
4.3.2.1 Example	402
4.3.3. Subscription	405
4.3.3.1 Example	406
4.4. System	408
4.4.1. Settings	408
4.4.2. Log Database	409
Chapter 5 Configuration Examples.....	411
5.1. Deployment and Configuration	411
5.1.1. Router Interface Configuration	411
5.1.2. Transparent Interface Configuration	417
5.1.2.1 Access Interface Configuration	417
5.1.2.2 Trunk Interface Configuration	419
5.1.3. Virtual Wire Interface Configuration	425
5.1.4. Bypass Mirror Interface Configuration.....	427
5.1.5. Subinterface Configuration	432
5.1.6. Hybrid Deployment	435
5.2. Policy Based Routing Configuration	439
5.2.1. Example 1	439

5.2.2. Example 2	441
5.3. ARP Proxy Configuration	444
5.4. DHCP Configuration	445
5.4.1. Server Configuration.....	445
5.4.2. DHCP Relay Configuration	447
5.5. Configuration of DoS/DDoS Protection	448
5.6. Access Control Configuration.....	452
5.6.1. Configuration of Application Control Policy	452
5.6.2. URL Filter Configuration.....	455
5.6.3. File Type Filter Configuration	457
5.7. IPS Configuration	459
5.8. Configuration of Web Application Protection.....	463
5.8.1. Example 1: WAF.....	463
5.8.2. Example 2: Data Leak Protection	468
5.9. Website Anti-defacement Configuration.....	472
5.10. Risk Assessment	479
5.11. Hot Standby Application	488
5.11.1. Example 1	488
5.11.2. Example 2	494
Appendix: SANGFOR NGAF Upgrade System.....	497

About This Document

Organization

- Part I Introduces the installation guide to the NGAF product of SANGFOR. This part describes the appearance, functions, and performance specifications of the NGAF equipment, and preparations and precautions for its connection.
- Part II Introduces how to use and log in to the NGAF console.
- Part III Introduces the functions of the NGAF equipment.
- Part IV Introduces the functions of the NGAF data center.
- Part V Introduces a set of cases. This part describes typical configuration cases of functional modules under a common environment.



This document takes SANGFOR NGAF5100 as an example. Equipment of different models differs in both hardware and software specifications. Therefore, confirm with SANGFOR about problems involving product specifications.

Conventions

GUI Conventions

Item	Sign	Example
Button	Frame+Shadow+Shading	The OK button can be simplified as OK .
Menu item	{ }	The menu item System Setup can be simplified as System Setup .
Choose cascading menu items	→	Choose System Setup > Interface Configuration .
Drop-down list, option button, check box	[]	The Enable User check box can be simplified as Enable User .
Window name	Bold Font	Open the New User window.
Prompt	“ ”	The prompt “Succeed in saving configuration. The configuration is modified. You need to restart the DLAN service for the modification to take effect. Restart the service now?” is displayed.

Symbol Conventions

The symbols that may be found in this document are defined as follows:



Caution: alerts you to a precaution to be observed during operation. Improper operation may cause setting validation failure, data loss, or equipment damage.



Warning: alerts you to pay attention to the provided information. Improper operation may cause bodily injuries.



Note or tip: provides additional information or a tip to operations.

Technical Support

Email: tech.support@sangfor.com.hk

International Service Centre: +60 12711 7129 (7511) Malaysia: 1700817071

Website: www.sangfor.com

Acknowledgement




Thanks for choosing our product and user manual. For any suggestions on our product or user manual, provide your feedback to us by phone or email.

Installation Guide

This part describes the composition and hardware installation of the NGAF series products of SANGFOR. You can configure and commission the product after the hardware is correctly installed.

1.1. Environment Specifications

The environment specifications of the SANGFOR NGAF equipment are listed as follows:

-  Input voltage: 110-230 V
-  Temperature: 0-45°C
-  Humidity: 5%-90%

Take proper grounding and dustproof measures, and keep good ventilation and stable room temperature in the application environment to ensure long-term and stable operation of the system. The product complies with the design requirements in terms of environment protection. The deployment, application, and scrapping of the product must be in accordance with national laws and regulations.

Power Supply

The SANGFOR NGAF series products are supplied with 110-230 V AC power. Before connecting power to the product, ensure that proper grounding measures are taken for the power supply.

Appearance



Figure 1 Front panel (NGAF M5100)

1. CONSOLE interface 2.USB 3. MANAGE interface 4.ETH3
5. ETH2 6.ETH1



The ALARM indicator is steady on in red during startup of the equipment. If the indicator turns off after 1-2 minutes, the equipment is started properly. If the indicator does not turn off for a long period of time, power off the equipment and then start it again after 5 minutes. If the problem persists, contact the

customer service center to confirm whether the equipment is damaged. After the equipment is started properly, the ALARM indicator may blink in red sometimes. This means that the equipment is writing system logs.



The **CONSOLE** interface is used only for development and commissioning. End users connect to the equipment through the **CONSOLE** interface.

Configuration and Management

Before configuring the equipment, get a computer ready and ensure that the webpage browser (such as the Internet Explorer) installed on the computer works properly. Then connect the computer to the same local area network (LAN) as the SANGFOR NGAF equipment and configure the equipment.

The management interface of the NGAF equipment is **MANAGE (ETH0)** and its default IP address is 10.251.251.251/24. Connect the **MANAGE (ETH0)** interface to the LAN or directly to the computer by using a network cable at initial login.

Equipment Connection

Connect the power cable on the backplane and turn on the power switch. Then the **POWER** indicator (green) and **ALARM** indicator (red) on the front panel becomes on. The **ALARM** indicator turns off in 1-2 minutes, which indicates that the gateway works properly.

Connect the **MANAGE (ETH0)** interface to the LAN by using a network cable with an RJ-45 connector and then configure the NGAF equipment.

After logging in to the console, perform network connection and connect cables based on the network environment and deployment requirements. For details, see section 3.2.



When the equipment works properly, the **POWER** and **LINK** indicators are steady on. The **ACT** indicator blinks in case of data flows. The **ALARM** indicator (red) is on for about 1 minute at startup due to system loading, and is off in normal operation. If the **ALARM** indicator is steady on during installation, power off the equipment and then start it again. If the problem persists, contact SANGFOR.



Use a straight-through cable to connect the network interface directly to a modem or switch, and a crossover cable to connect network interface to a router. If the indicators are normal but the cable connection fails, check whether a wrong network cable is used. A straight-through cable differs from a cross-over cable in the wire sequence at both ends. See the figure below.

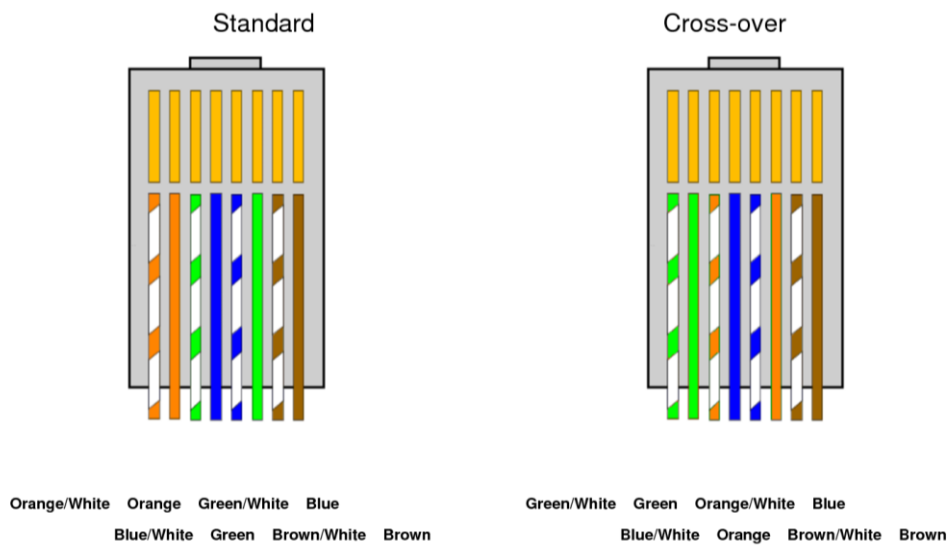


Figure 2 Wire sequences of straight-through cables and cross-over cables

Introduction to the Console

Logging In to the Web UI

The NGAF equipment supports Hypertext Transfer Protocol Secure (HTTPS) login through a standard HTTPS port. If you log in through the MANAGE interface at initial login, the URL is <https://10.251.251.251>.

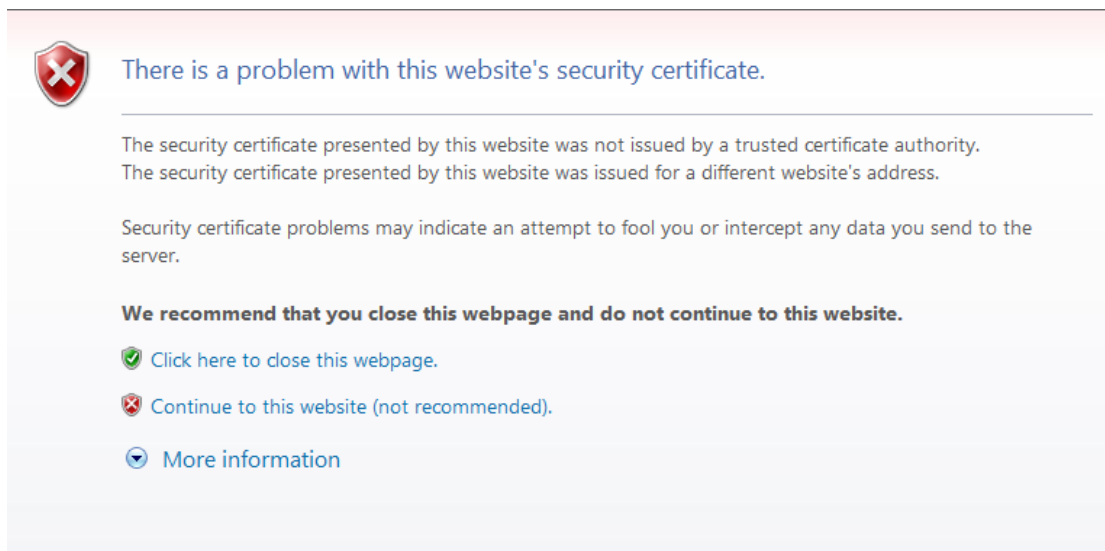


Login to the Web UI of the NGAF equipment through HTTPS can avoid security threats caused if the configurations are intercepted during transmission.

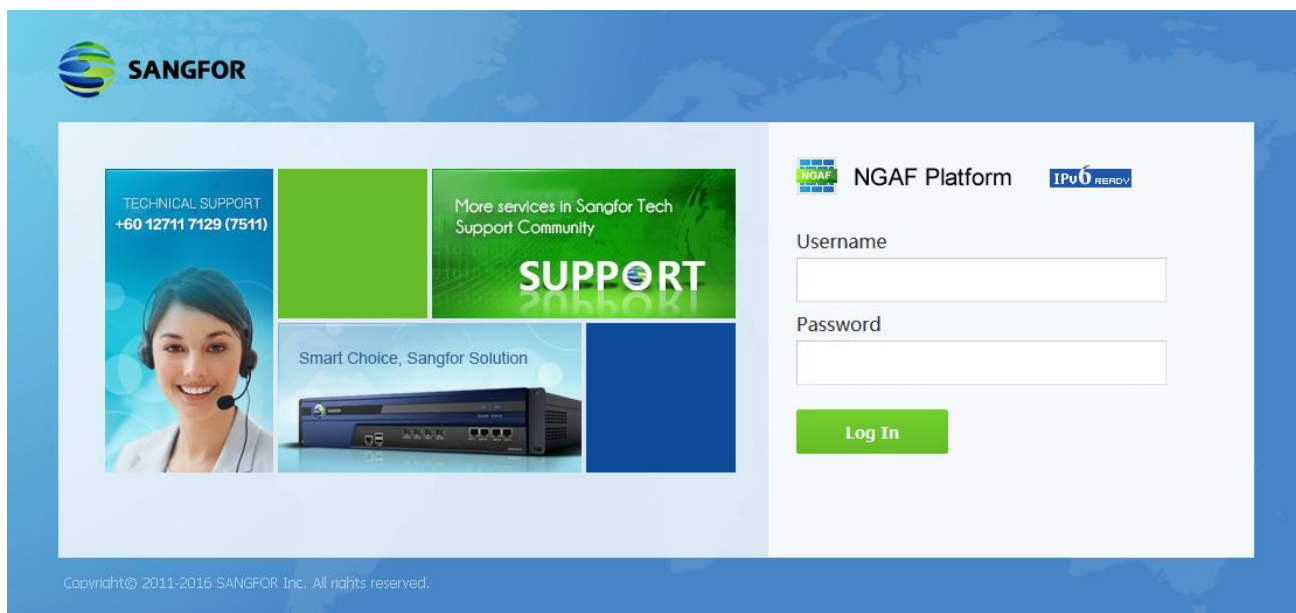
How to log in to the console page of the NGAF equipment?

Connect the cables as described earlier and then configure the NGAF equipment on the Web UI. The procedure is as follows:

Configure an IP address (10.251.251.100 for example) on the 10.251.251.X network segment for the computer from which you log in to the console. Then enter the default login IP address and port number of the MANAGE interface on the address bar of the Internet Explorer, that is, <https://10.251.251.251>. A safety prompt shown in the figure below is displayed.



Click **Yes** and the login interface shown in the figure below is displayed.

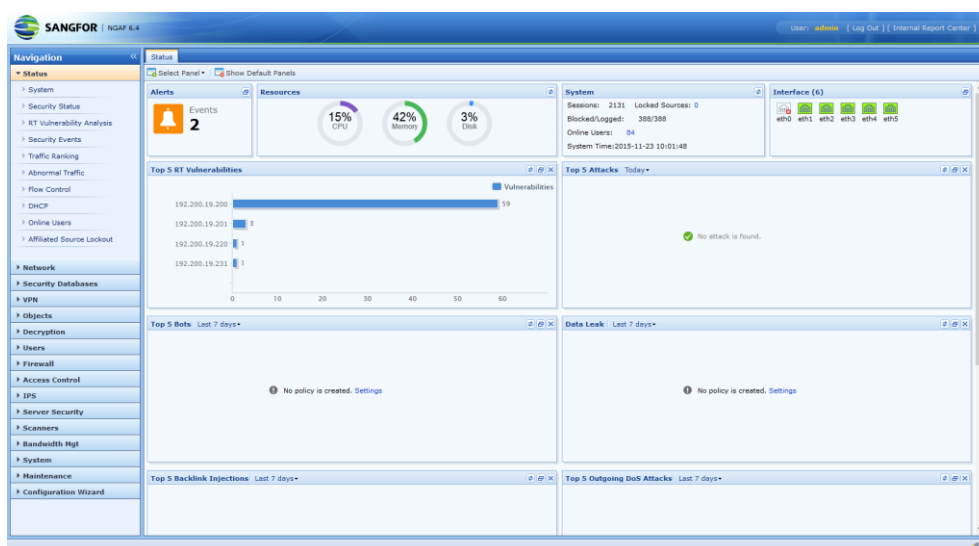



Enter the user name and password and click **Log In**. the default user name and password are both **admin**.


You do not need to install any control for logging in to the console. You can log in to the console by using another browser instead of the Internet Explorer.

Configuring and Using the Console

After logging in to the configuration Web UI, you can view the following configuration modules: Status, Network, Security Databases, VPN, Objects, Authentication, Firewall, Access Control, IPS, Server Security, Risk Assessment, Bandwidth Mgt, System, Maintenance, and Configuration Wizard.



The icon  in the lower right corner of the console is used to notify system information and alarm information about the equipment in real time.

When you hover the pointer over the icon  on any configuration page, the brief help information about the current configuration item is displayed. This part is not described in the following sections.

Function Description

Status

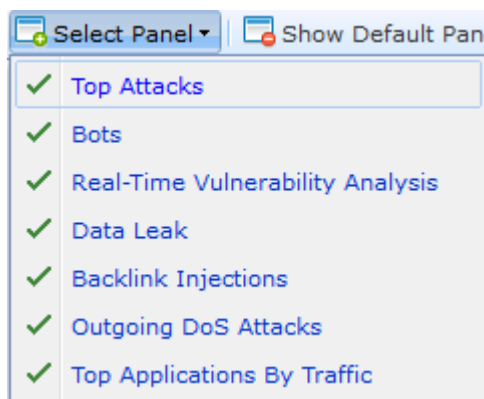
The **Status** configuration module displays basic status information about the equipment, including **System Status**.

System Status

The **System Status** page displays alerts, resources, system, interfaces information, Top 5 RT Vulnerabilities, Top 5 Attacks, Top 5 Bots, Data Leak, Top 5 Backlink Injections, Top 5 Outgoing DoS Attacks and Top Applications By Traffic – All lines Bidirectional.

Selecting Panels

On the **System Status** page, click **Select Panel**. The following page is displayed:



Select the status information to be displayed on the **System Status** page.

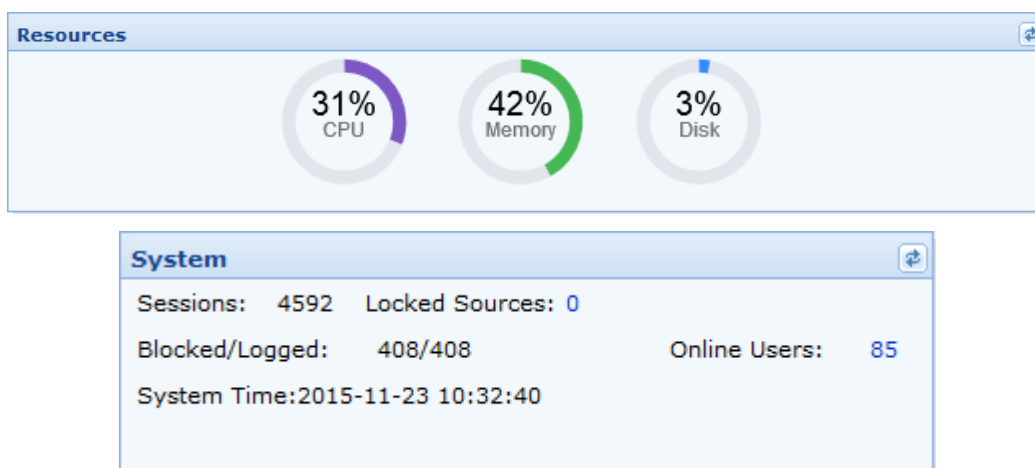
Showing Default Panels

On the **Status** page, click **Show Default Panels** and the default panels are displayed, including **Alerts, Resources, System, Interface, Top 5 RT Vulnerabilities, Top 5 Attacks, Top 5 Bots, Data Leak, Top 5 Backlink Injections, Top 5 Outgoing DoS Attacks** and **Top Applications By Traffic – All lines Bidirectional**.

Viewing Status

3.1.1.3.1 System Status

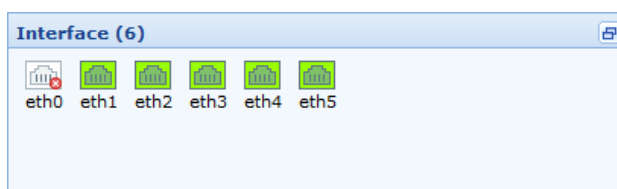
The **System Status** page displays the overall conditions of system resources, including the CPU usage, memory usage, disk usage, number of sessions, number of online users, system time, and information about Locked Sources and Blocked/Logged actions. See the figure below.



The information will automatically refresh every 5 seconds.

3.1.1.3.2 Interface

The **Interface** page displays the status and cable connection of each network interface. See the figure below.



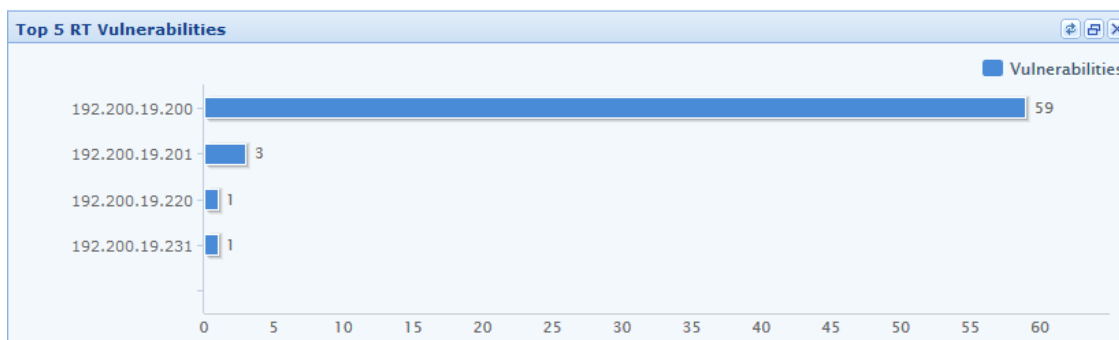
Indicates that a network interface is in the **connected** state.



Indicates that a network interface is in the **disconnected** state.

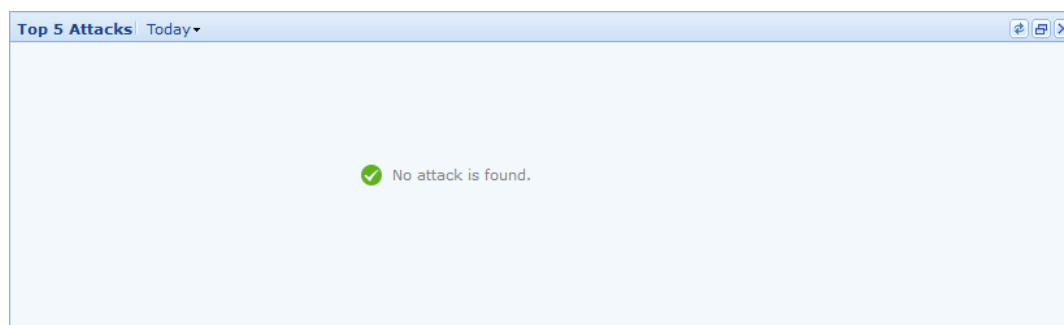
3.1.1.3.3 Top 5 RT Vulnerabilities

The **Top 5 RT Vulnerabilities** page displays the overall information about server vulnerabilities, vulnerable servers. See the figure below.

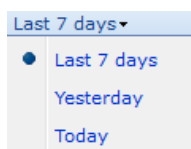


3.1.1.3.4 Top 5 Attacks

The **Top 5 Attacks** page displays attack events that occurs in the network.



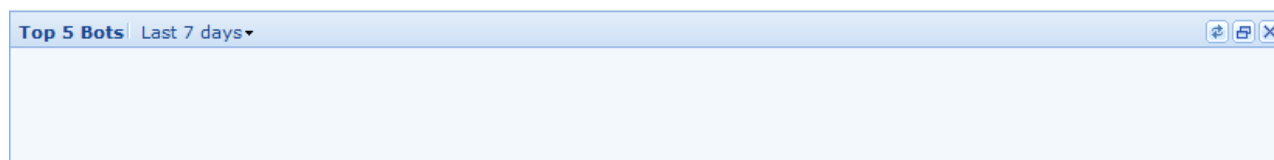
You can select



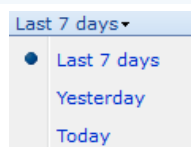
to display different day result.

3.1.1.3.5 Top 5 Bots

The **Top 5 Bots** page displays the top 5 Bots that attack the network in the last 7 days. See the figure below.



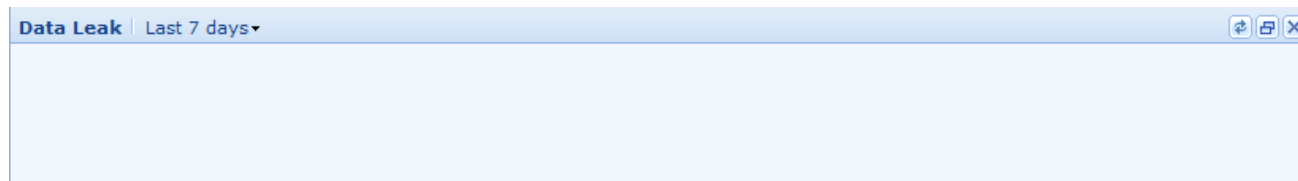
You can select

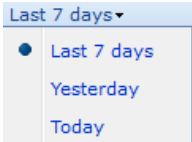


to display different day result.

3.1.1.3.6 Data Leak

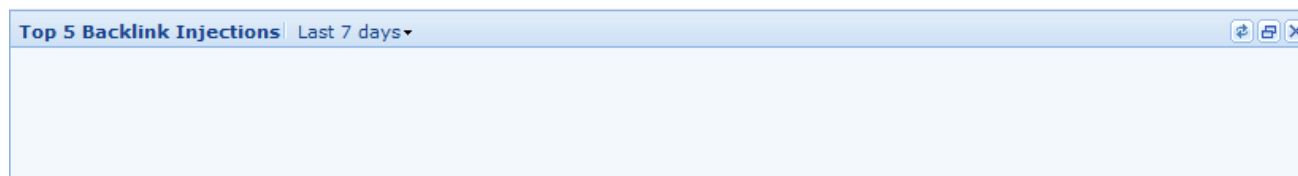
The **Data Leak** page displays any data leakage in the last 7 days. See the figure below.

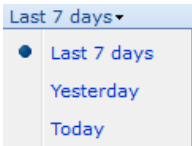


You can select  to display different day result.

3.1.1.3.7 Top 5 Backlink Injections

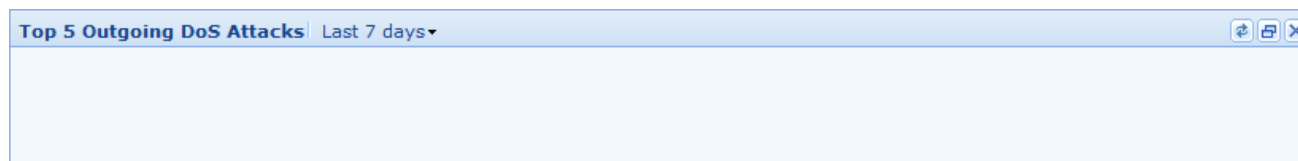
The **Top 5 Backlink Injections** page displays the backlink injection attacks in last 7 days. See the figure below.

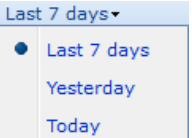


You can select  to display different day result.

3.1.1.3.8 Top 5 Outgoing DoS Attacks

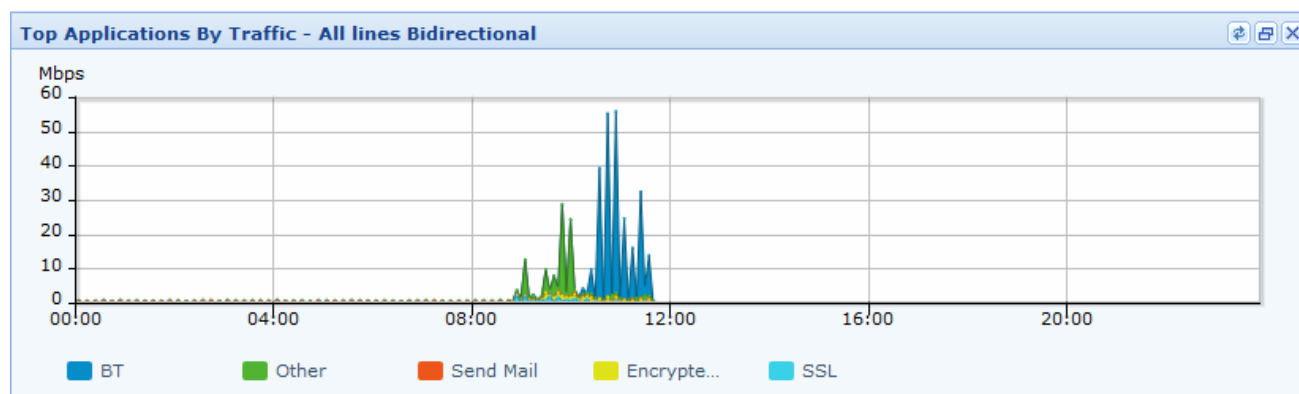
The **Top 5 Outgoing DoS Attacks** page displays outgoing DoS attacks in the last 7 days. See the figure below.



You can select  to display different day result.

3.1.1.3.9 Top Applications By Traffic – All lines Bidirectional

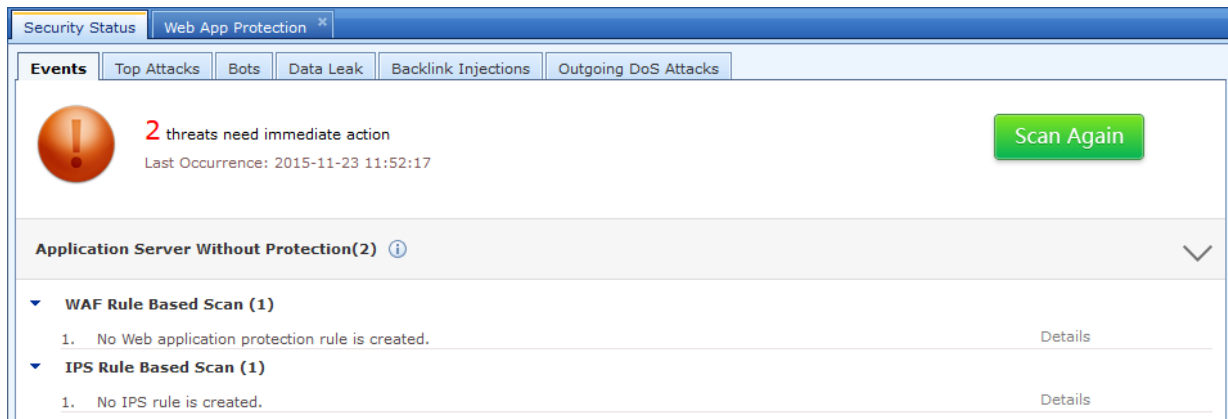
The **Top Applications By Traffic – All lines Bidirectional** page displays the traffic speed trends of applications dynamically in different colors. See the figure below.



Security Status

Events

The **Events** page displays current threat and information about the threats.

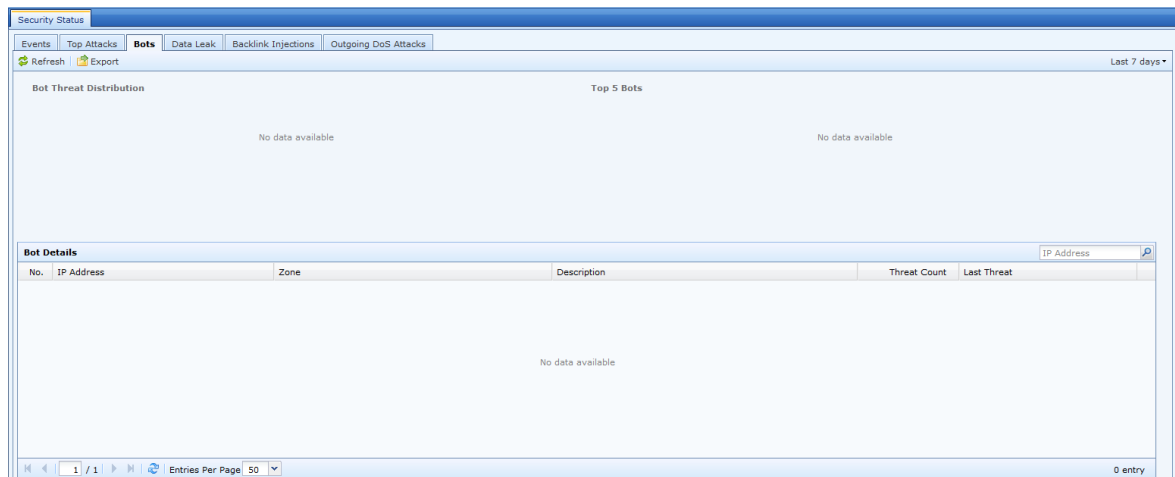


Click **Scan Again** to scan the servers for threats.

Click **Details** to display more information.

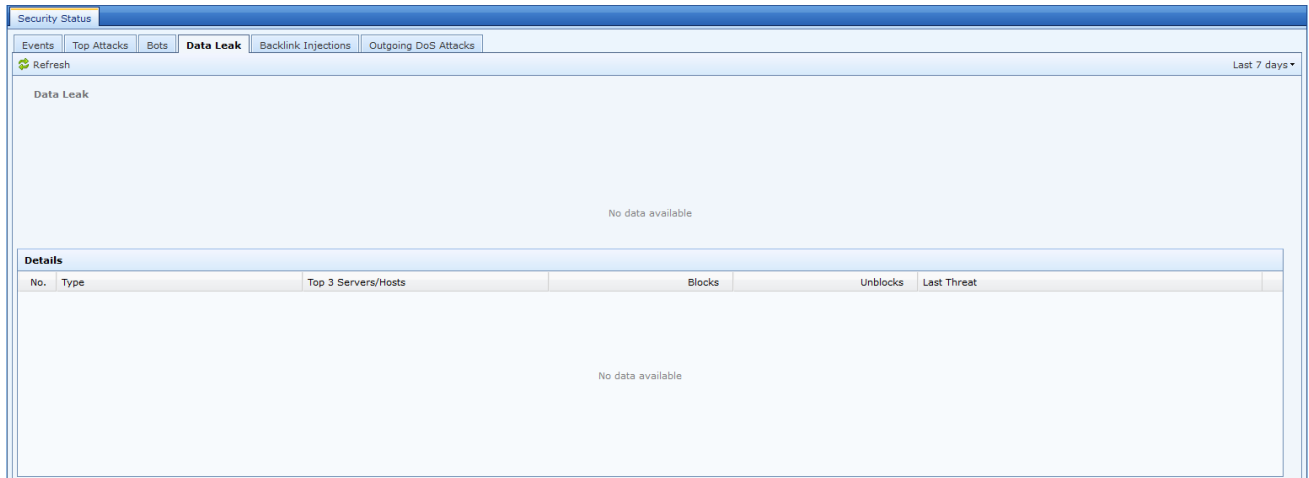
Bots

The **Bots** page displays current top 5 Bots and information about the Bots.



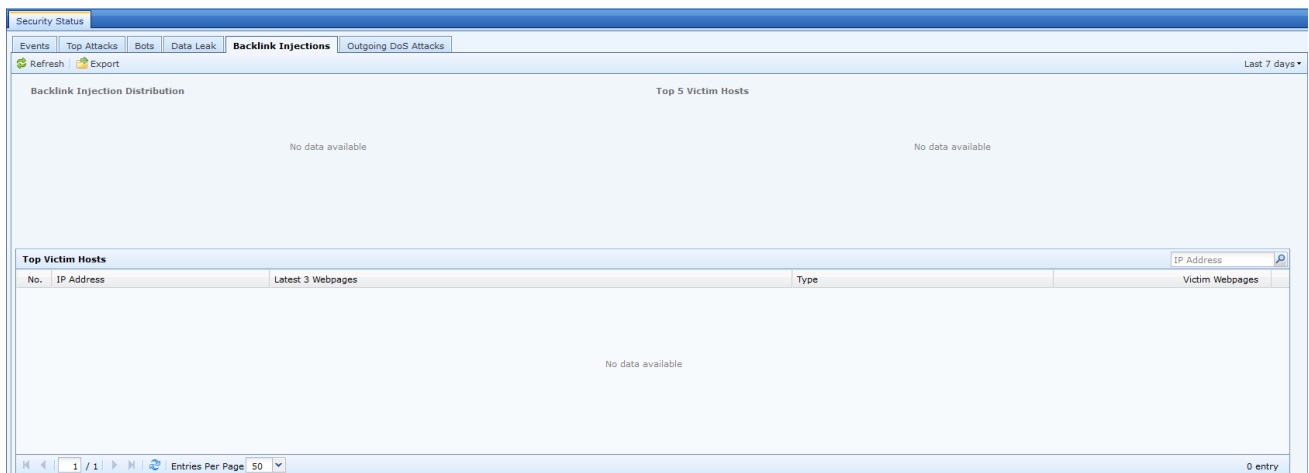
Data Leak

The **Data Leak** page displays any data leakage and information about the Data Leak.



Backlink Injections

The **Backlink Injections** page displays any backlink injections occur in the network and information about the Backlink Injections.



Outgoing DoS Attacks

The **Outgoing DoS Attacks** page displays any outgoing DoS attacks occur in the network and information about the outgoing DoS attacks.

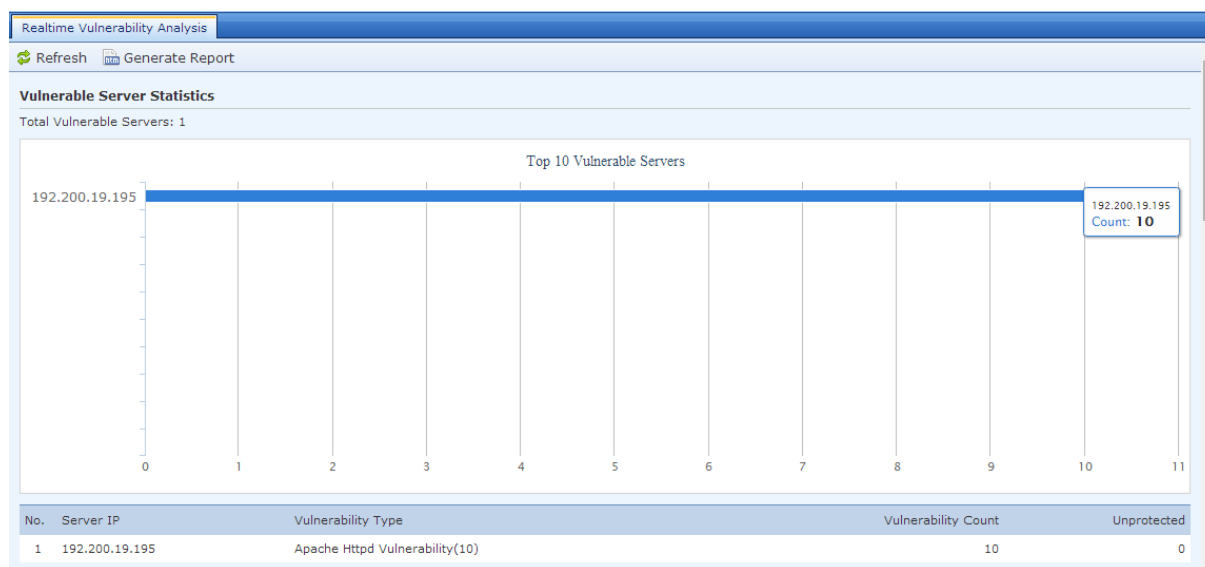
The screenshot shows a web-based security management interface. At the top, there is a 'Security Status' tab. Below it, a navigation bar includes tabs for 'Events', 'Top Attacks', 'Bots', 'Data Leak', 'Backlink Injections', and 'Outgoing DoS Attacks'. The 'Outgoing DoS Attacks' tab is active. A 'Refresh' button and a 'Last 7 days' filter are located on the right. The main content area is divided into two sections: 'Top 5 Attack Sources from LAN' and 'Top 5 Destinations'. Both sections display 'No data available'. Below these is a 'Details' section with a table header: 'No.', 'Started Since', 'Duration', 'Attack Source', 'Destination IP', and 'Logging'. The table body is empty, showing 'No data available'. At the bottom, there is a pagination bar with '1 / 1' and 'Entries Per Page 50'. The bottom right corner indicates '0 entry'.

No.	Started Since	Duration	Attack Source	Destination IP	Logging
No data available					

RT Vulnerabilities Analysis

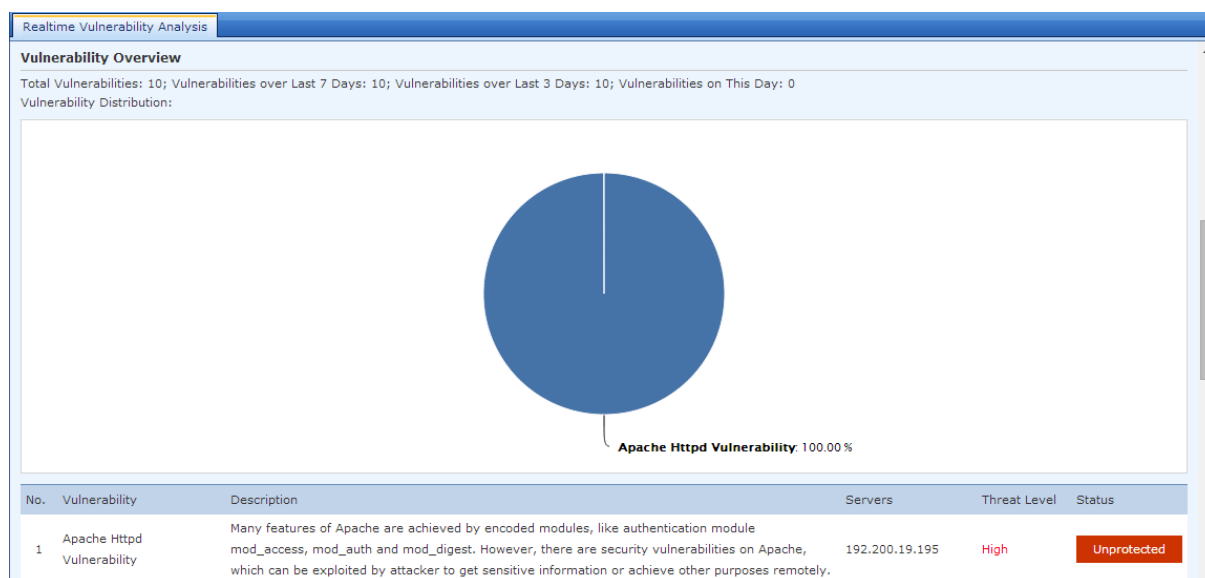
Viewing RT Vulnerabilities Analysis

The **RT Vulnerabilities Analysis** page displays real time vulnerable server statistic, vulnerability overview, latest critical vulnerabilities and latest vulnerabilities. See the figure below.



Click **Refresh** to refresh the information immediately.

Click **Generate Report** to generate a detailed report with full information



Realtime Vulnerability Analysis							
Latest Critical Vulnerabilities							
No.	Type	Vulnerability	Servers	Time Announced	Threat Level	Status	Solution
No data available							
Latest Vulnerabilities							
				Last 7 Days		Last 30 Days	
No.	Time Last Detected	Vulnerability	Servers	Threat Level	Status	Details	
1	2014-08-28 16:52:25	Apache 2.2 < 2.2.20 Multiple Vulnerabilities	192.200.19.195	High	Potential Risk	View	
2	2014-08-28 16:52:25	Apache HTTP Server denial of service	192.200.19.195	High	Potential Risk	View	
3	2014-08-28 16:52:25	Apache HTTP Server vulnerability in the mod_session_dbd module	192.200.19.195	High	Potential Risk	View	
4	2014-08-28 16:52:25	Version later than Apache 2.2 and earlier than 2.2.22 allows unauthorized information disclosure	192.200.19.195	Medium	Potential Risk	View	
5	2014-08-28 16:52:25	Version later than Apache 2.2 and earlier than 2.2.22 allows attackers to cause denial of service	192.200.19.195	Medium	Potential Risk	View	
6	2014-08-28 16:52:25	Version later than Apache 2.2 and earlier than 2.2.22 allows heap-based buffer overflow	192.200.19.195	Medium	Potential Risk	View	
7	2014-08-28 16:52:25	Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilities	192.200.19.195	Medium	Potential Risk	View	
8	2014-08-28 16:52:25	Apache 2.2 < 2.2.23 Multiple Vulnerabilities	192.200.19.195	Medium	Potential Risk	View	
9	2014-08-28 16:52:25	Version later than Apache 2.2 and earlier than 2.2.22 has vulnerability	192.200.19.195	Medium	Potential Risk	View	

Click **View** to read on the vulnerability details and suggestion of solutions.

Security Events

Security Event

Recent Security Events

Server Security

Endpoint Security

Recent Attack Sources

Refresh: 5 seconds

Refresh

No.	Time	Src IP	Dst IP	Attack Type	URL	Description	Action	Details
-----	------	--------	--------	-------------	-----	-------------	--------	---------

Recent Security Events

The **Recent Security Events** page displays recent attack events. See the figure below.

Recent Security Events									
Server Security		Endpoint Security		Recent Attack Sources					
Refresh: 5 seconds ▾ Refresh									
No.	Time	Src IP	Dst IP	Attack Type	URL	Description	Action	Details	

The displayed information includes the attack time, source IP address, destination IP address, attack type, and attacked URL.

Click **Refresh: 5 seconds** to set the refresh interval.

Click **Refresh** to refresh the information immediately.

Server Security

The **Sever Security** page displays the types of attacks suffered by target servers. See the figure below.

Recent Security Events

Server Security

Endpoint Security

Recent Attack Sources

Refresh: 5 seconds

Refresh

No.	Time	Target Server	Description	URL	Attack Type	Details
-----	------	---------------	-------------	-----	-------------	---------

The displayed information includes the attack time, target server, URL, attack type, and attack details.

Click **Refresh: 5 seconds** to set the refresh interval.

Click **Refresh** to refresh the information immediately.

Endpoint Security

The **Endpoint Security Events** page displays the types of attacks suffered by the end users. See the figure below.

Recent Security Events

Server Security

Endpoint Security

Recent Attack Sources

Refresh: 5 seconds

Refresh

No.	Time	Host IP	Username	Group	Attack Type	Details
-----	------	---------	----------	-------	-------------	---------

The displayed information includes the attack time, host IP address, user name, group, attack type, and attack details.

Click **Refresh: 5 seconds** to set the refresh interval.

Click **Refresh** to refresh the information immediately.

Recent Attack Sources

The **Recent Attack Sources** page displays the sources of recent attack events. See the figure below.

Recent Security Events

Server Security

Endpoint Security

Recent Attack Sources

Refresh: 5 seconds

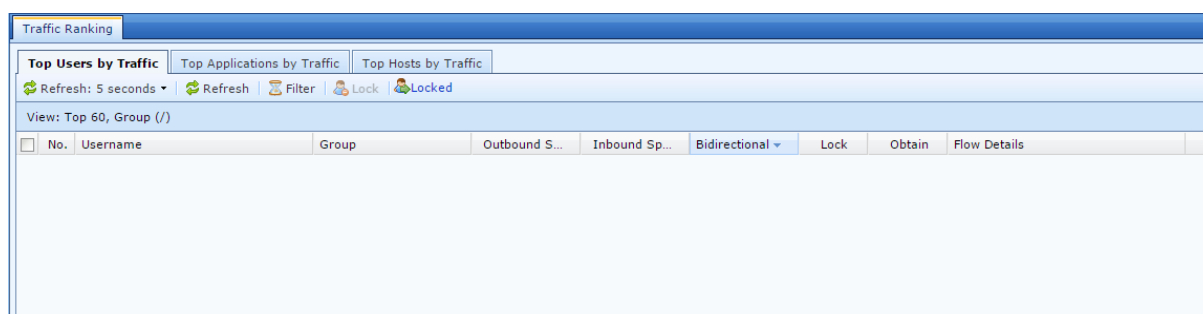
Refresh

No.	Time	Attack Source	Attack Type	Details

The displayed information includes the attack time, attack source, attack type, and attack details.

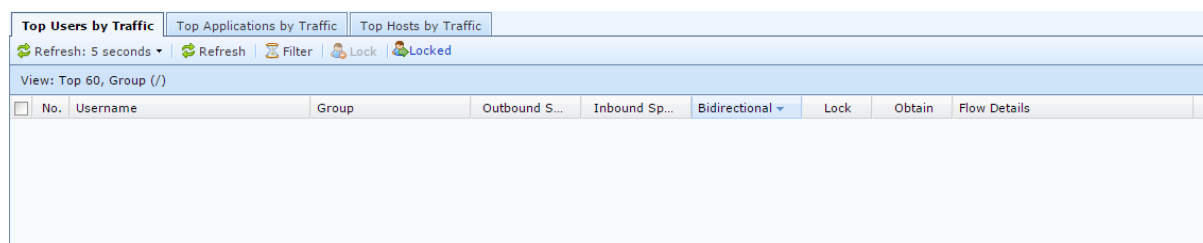
Click **Refresh: 5 seconds** to set the refresh interval. Click **Refresh** to refresh the information immediately.

Traffic Ranking



Top Users by Traffic

The **Top Users by Traffic** page displays the bandwidth usage of online hosts. See the figure below.



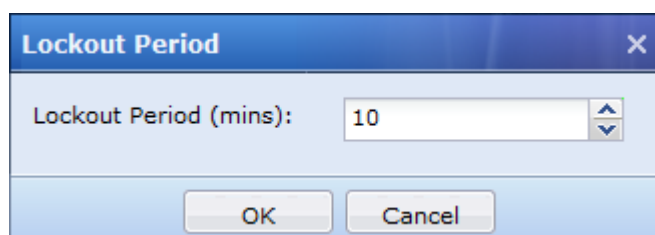
The Users are ranked by traffic. The displayed information includes the username, group, outbound speed, inbound speed, bidirectional speed, lock, link for obtaining the computer name, and flow details. In the **Obtain** column, click **Obtain** to obtain the computer name corresponding to the IP address. In the **Flow Details** column, click an application to display the traffic information about the corresponding host. See the figure below.

Application	Line	Percent	Outbound	Inbound	Bidirectional
SSL	-	66%	12.23(Kb/s)	44.09(Kb/s)	56.31(Kb/s)
Website Browsing	-	20%	9.88(Kb/s)	6.88(Kb/s)	16.75(Kb/s)
Other	-	9%	4.91(Kb/s)	2.48(Kb/s)	7.39(Kb/s)
DNS	-	4%	1.32(Kb/s)	2.43(Kb/s)	3.75(Kb/s)
NETBIOS	-	1%	880(b/s)	0(b/s)	880(b/s)

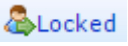
Click **Refresh: 5 seconds** to set the refresh interval.

Click **Refresh** to refresh the information immediately.

Click **Lock** or  in the **Operation** column. The page shown in the figure below is displayed.

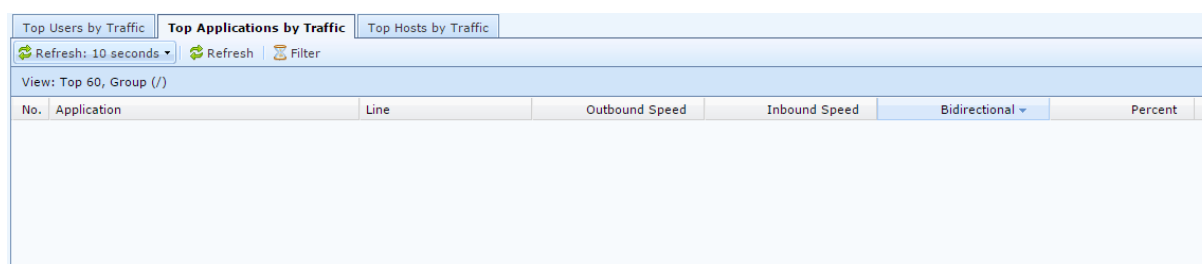


After setting the **Lockout Period**, click **OK**.

Click  icon in the **Operation** column to open **Online Users** page to unlock locked users.

Top Applications by Traffic

The **Top Applications by Traffic** page displays rankings of applications by traffic in real time. See the figure below.



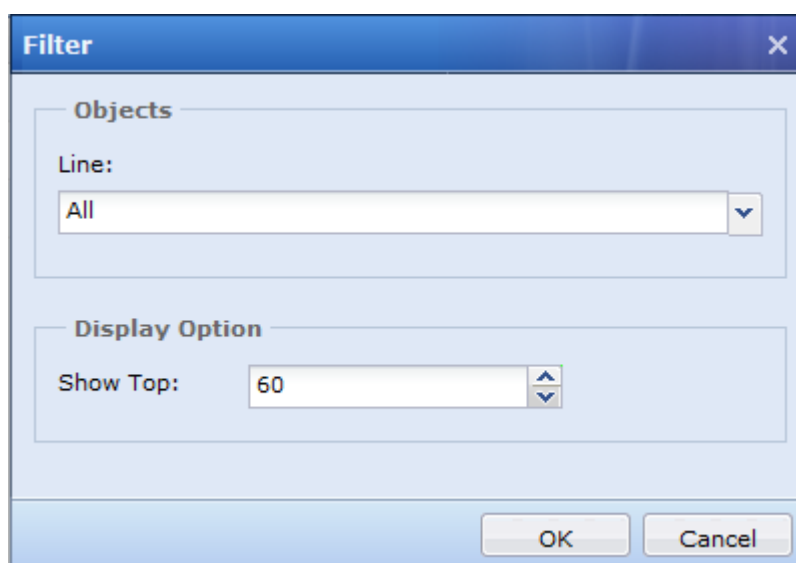
No.	Application	Line	Outbound Speed	Inbound Speed	Bidirectional	Percent
-----	-------------	------	----------------	---------------	---------------	---------

The applications are ranked by occupied bandwidth. The displayed information includes the application type, line, outbound speed, inbound speed, and bidirectional speed.

Click **Refresh: 5 seconds** to set the refresh interval.

Click **Refresh** to refresh the information immediately.

Click **Filter** to specify the conditions for filtering applications by traffic. See the figure below.



Filter

Objects

Line:

Display Option

Show Top:

OK Cancel

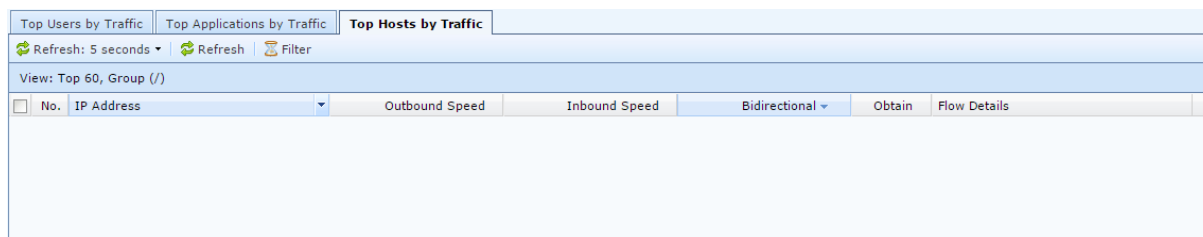
Set the line to be viewed in the **Objects** pane.

Select a value from the **Line** drop-down list.

In the **Display Option** pane, you can set the number of displayed applications ranked by traffic.

Top Hosts by Traffic

The **Top Hosts by Traffic** page displays the bandwidth usage of online hosts. See the figure below.



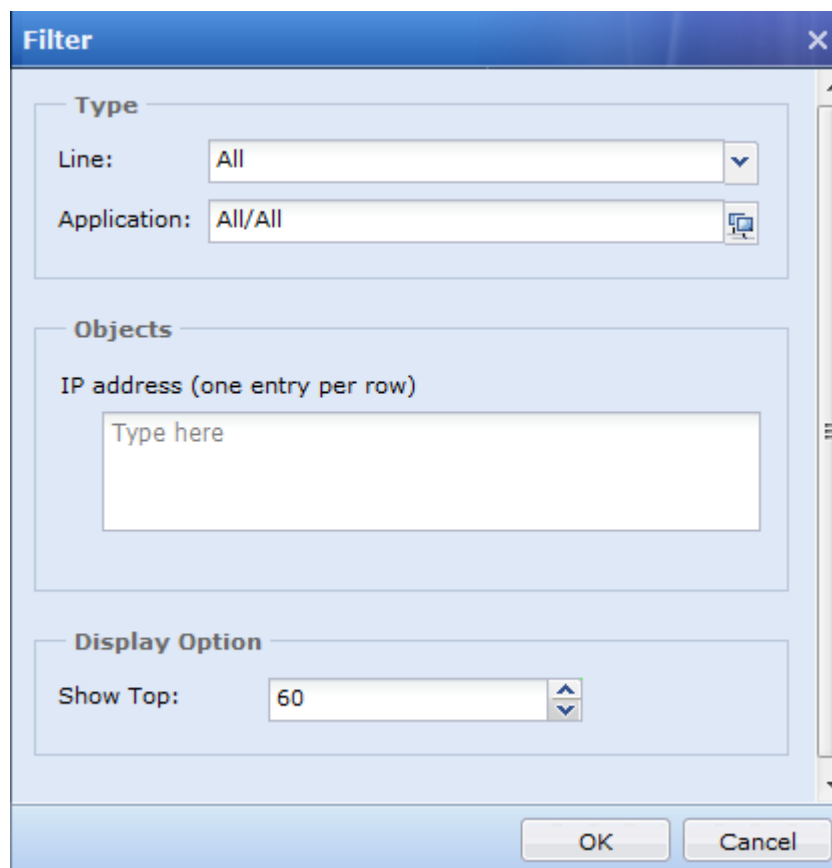
The hosts are ranked by traffic. The displayed information includes the IP address, outbound speed, inbound speed, bidirectional speed, link for obtaining the computer name, and flow details. In the **Obtain** column, click **Obtain** to obtain the computer name corresponding to the IP address. In the **Flow Details** column, click an application to display the traffic information about the corresponding host. See the figure below.

Application	Line	Percent	Outbound	Inbound	Bidirectional	
SSL	-	66%	12.23(Kb/s)	44.09(Kb/s)	56.31(Kb/s)	
Website Browsing	-	20%	9.88(Kb/s)	6.88(Kb/s)	16.75(Kb/s)	
Other	-	9%	4.91(Kb/s)	2.48(Kb/s)	7.39(Kb/s)	
DNS	-	4%	1.32(Kb/s)	2.43(Kb/s)	3.75(Kb/s)	
NETBIOS	-	1%	880(b/s)	0(b/s)	880(b/s)	

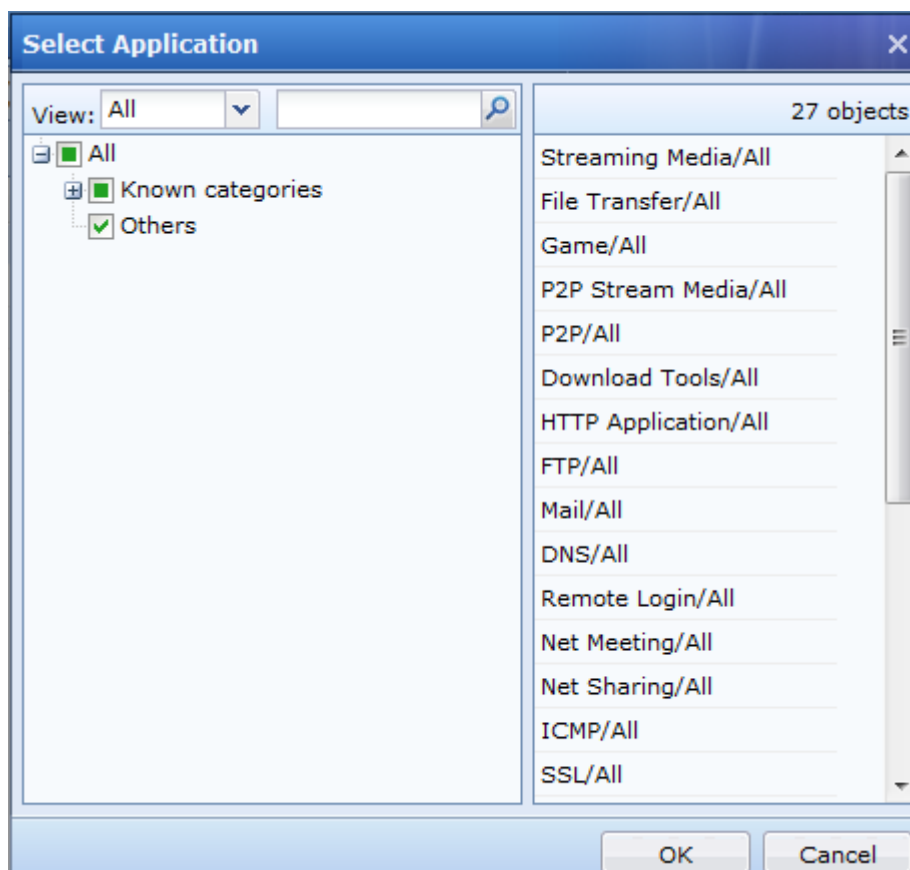
Click **Refresh: 5 seconds** to set the refresh interval.

Click **Refresh** to refresh the information immediately.

Click **Filter** to specify the conditions for filtering hosts by traffic. See the figure below.



Set the line and application in the **Type** pane. **Line** specifies the line to be viewed and **Application** specifies the application to be viewed. After setting the line and application, click **OK**. The page shown in the figure below is displayed.



You can choose to display all applications, selected applications and unselected applications. The selected applications are displayed in the right pane. Click **OK** to save the settings.

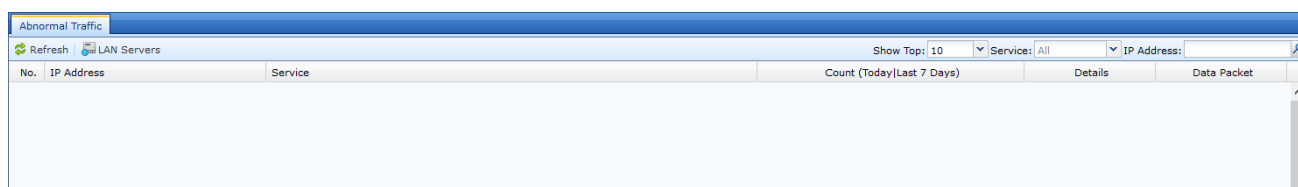
Objects specifies a specific IP address.

In the **Display Option** pane, you can set the number of displayed IP addresses ranked by traffic.

Abnormal Connection

The **Abnormal Connection** page shows abnormal connection from attacker which uses common ports number to forward traffics with another protocol.

For example, if NGAF detects SSL traffics forward in port 53, NGAF take action of these connections based on user configuration because by default port 53 is used by DNS protocol but attackers exploited it.



Click **Refresh** to refresh the information immediately.

Click **LAN Servers** to display manual added servers or auto identified servers by NGAF. See the figure below.

Abnormal Traffic LAN Servers					
+ Add - Delete Refresh					
<input type="checkbox"/>	No.	Server IP	Service & Port	Description	Operation
Custom Servers					
<input type="checkbox"/>	1	192.200.19.200	Web(808,80,8080,8081); FTP(21); Database(1433); Email(808)	TSC	Delete
Auto Identified Servers					
-	1	192.200.19.201	Web(80)	-	Excluded
-	2	192.200.19.220	LDAP(389)	-	Excluded
-	3	192.200.19.227	Web(85)	-	Excluded
-	4	192.200.19.228	Web(80)	-	Excluded
-	5	192.200.19.229	Web(80)	-	Excluded
-	6	192.200.19.231	Web(80)	-	Excluded
-	7	192.200.19.232	Web(800)	-	Excluded

Flow Control

The **Flow Control** page displays real-time traffic information about channels for which traffic management is enabled. See the figure below.

Flow Control

Refresh: 5 seconds

Refresh

BM System Status: Running

Configure BM

WAN Speed

Name	Transient Speed	Speed History	Max Speed Allowed	Percent	Traffic History
Line 1	↑ 331.61(Kb/s) ↓ 282.2(Kb/s)	↑ 177.52(Kb/s) ↓ 172.51(Kb/s)	↑ 5(Mb/s) ↓ 5(Mb/s)	↑ 6% ↓ 5%	↑ 52.01(MB) ↓ 50.54(MB)
Line 2	↑ 288.01(Kb/s) ↓ 2.26(Mb/s)	↑ 261.8(Kb/s) ↓ 2.77(Mb/s)	↑ 20(Mb/s) ↓ 20(Mb/s)	↑ 1% ↓ 11%	↑ 76.7(MB) ↓ 830.78(MB)
Total rate	↑ 619.62(Kb/s) ↓ 2.53(Mb/s)	↑ 439.32(Kb/s) ↓ 2.94(Mb/s)	↑ 25(Mb/s) ↓ 25(Mb/s)	↑ 2% ↓ 10%	↑ 128.71(MB) ↓ 881.32(MB)

Bandwidth Channel

Exclusion Rule

Tips: The two values in some columns respectively stand for Outbound ↑ / Inbound ↓

Period:

None

View:

All channels

Name	Line	Transient Speed	Percent	Users	Min Bandwidth	Max Bandwidth	Status
limit	Line 1	0(b/s) 0(b/s)	0% 0%	0	0(b/s) 0(b/s)	2.5(Mb/s) 2.5(Mb/s)	Running
BASIC	Line 1	161.43(Kb/s) 161.61(Kb/s)	3% 3%	0	2.5(Mb/s) 2.5(Mb/s)	4(Mb/s) 4(Mb/s)	Running
Default channel	All	458.19(Kb/s) 2.38(Mb/s)	1% 9%	-	0(b/s) 0(b/s)	25(Mb/s) 25(Mb/s)	Running

Click **Refresh: 5 seconds** to set the refresh interval.

Click **Refresh** to refresh the information immediately.

BM System Status in the upper part of the **Flow Control** page indicates whether the bandwidth management system is started. You can view real-time traffic information about channels only when the bandwidth management system is in the **Running** state.

Click **Configure BM** to open the **Bandwidth Management** page.

WAN Speed

WAN Speed						
Name	Transient Speed	Speed History	Max Speed Allowed	Percent	Traffic History	
Total rate	↑ 144.98(Kb/s) ↓ 40.33(Kb/s)	↑ 116.92(Kb/s) ↓ 35.24(Kb/s)	↑ 5(Mb/s) ↓ 5(Mb/s)	↑ 0% ↓ 0%	↑ 4.96(MB) ↓ 10.32(MB)	

The **WAN Speed** pane displays the overall traffic conditions, including the transient speed, historical speed, preset speed, percentage, and historical traffic of each line and the main line.

Bandwidth Channel

The **Bandwidth Channel** tab page displays the traffic information about channels. See the figure below.

Bandwidth Channel Exclusion Rule							
Tips: The two values in some columns respectively stand for Outbound↑ / Inbound↓							
				Period: None	View: All channels		
Name	Line	Transient Speed	Percent	Users	Min Bandwidth	Max Bandwidth	Status
Default channel	All	None	0% 0%	0	None	5(Mb/s) 5(Mb/s)	Running

The displayed information includes the channel name, line, transient speed, percentage, user quantity, minimum bandwidth, maximum bandwidth, and status. You can choose to display the traffic history within a certain period of time. Select **All channels** or **Running channels** from the **View** drop-down list.

Exclusion Rule

The **Exclusion Rule** tab page displays the traffic information filtered out by the exclusion rule. See the figure below.

Bandwidth Channel		Exclusion Rule		
No.	Name	Transient Speed	Speed History	Traffic History
1	Total rate	0	0	0

DHCP

The **DHCP** tab page displays the assigned IP with hostname, MAC address, time assigned and lease (minutes).

The **Current Status** is displaying the status of DHCP.

Click **Refresh** to update the new DHCP information. See the figure below.

DHCP					
Refresh	Assigned IP Addresses: 39		Current Status: Running		
No.	IP Address	Host Name	MAC Address	Time Assigned	Lease(minutes)
0	192.168.19.60	android-15bc9c9fabcaeb29	B4527DE5EA95	2015-11-23 16:37:25	120
1	192.168.19.59	android-b632047ae147bb39	5C0A5BC16EB2	2015-11-23 16:34:07	120
2	192.168.19.16	android-777715e901845da0	2008ED706888	2015-11-23 16:30:30	120

Online Users

Viewing Online Users

The **Online Users** page displays authenticated users that are online. See the figure below.

Online Users

Refresh: 5 seconds

Refresh

Filter

Lock

Unlock

Force to Logout

Search by Name

User Status: AllIP/Username: None

Groups

Fuzzy match

(31 users)

Default group(31 us

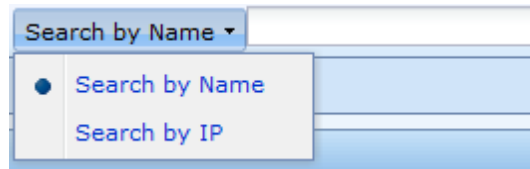
Users

	No.	Name(Display Name)	Group	IP Address	Authentication	Time Logged In/Locked	Online Duration	Operation
<input type="checkbox"/>	1	192.200.17.20	/Default ...	192.200.17.20	None	2013-8-6 16:54:35 Log In	17 hours 19 minutes ...	
<input type="checkbox"/>	2	192.200.17.200	/Default ...	192.200.17.200	None	2013-8-6 16:54:36 Log In	17 hours 19 minutes ...	
<input type="checkbox"/>	3	192.200.17.224	/Default ...	192.200.17.224	None	2013-8-6 16:54:36 Log In	17 hours 19 minutes ...	
<input type="checkbox"/>	4	192.200.17.118	/Default ...	192.200.17.118	None	2013-8-6 16:54:36 Log In	17 hours 19 minutes ...	
<input type="checkbox"/>	5	192.200.17.231	/Default ...	192.200.17.231	None	2013-8-6 16:54:36 Log In	17 hours 19 minutes ...	
<input type="checkbox"/>	6	192.200.17.236	/Default ...	192.200.17.236	None	2013-8-6 16:54:48 Log In	17 hours 19 minutes ...	
<input type="checkbox"/>	7	192.200.17.203	/Default ...	192.200.17.203	None	2013-8-6 16:54:55 Log In	17 hours 19 minutes ...	
<input type="checkbox"/>	8	192.200.17.221	/Default ...	192.200.17.221	None	2013-8-6 16:54:58 Log In	17 hours 19 minutes ...	
<input type="checkbox"/>	9	192.200.17.235	/Default ...	192.200.17.235	None	2013-8-6 16:55:06 Log In	17 hours 19 minutes ...	
<input type="checkbox"/>	10	169.254.56.212	/Default ...	169.254.56.212	None	2013-8-6 16:55:09 Log In	17 hours 18 minutes ...	
<input type="checkbox"/>	11	192.200.17.21	/Default ...	192.200.17.21	None	2013-8-6 17:50:48 Log In	16 hours 23 minutes ...	
<input type="checkbox"/>	12	169.254.65.88	/Default ...	169.254.65.88	None	2013-8-7 08:15:20 Log In	1 hour 58 minutes 48 ...	

The displayed information includes the name, group, IP address, authentication mode, login time or lockout time, online duration, and operation to be performed.

On the page, enter a keyword in the **Search** box to query online users of the corresponding user group.

On the **Online Users** page, you can search users by name or IP address. See the figure below.



Filtering Online Users

Click **Filter** to specify the conditions for filtering users. See the figure below.

User Status can be set to **All**, **Locked** or **Active**.


After selecting the **Objects** check box, you can filter users by user name or IP address. After setting the user name or IP address, click **OK**.

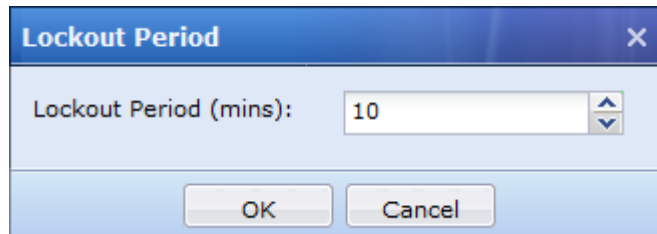
Locking Online Users

Select one or more users and click **Lock** to end the network connections of the selected users. The procedure is as follows:

Select a user.

Users								
<input type="checkbox"/>	No.	Name(Display Name)	Group	IP Address	Authentication	Time Logged In/Locked ▾	Online Duration	Operation
<input checked="" type="checkbox"/>	1	192.200.17.20	/Default ...	192.200.17.20	None	2013-8-6 16:54:35 Log In	17 hours 29 minutes ...	
<input type="checkbox"/>	2	192.200.17.231	/Default ...	192.200.17.231	None	2013-8-6 16:54:36 Log In	17 hours 29 minutes ...	

Click **Lock** or  in the **Operation** column. The page shown in the figure below is displayed.



After setting the **Lockout Period**, click **OK**. The status of the locked user changes, as shown in the figure below.

<input type="checkbox"/>	29	192.200.17.231	/Default ...	192.200.17.231	None	2013-8-7 10:25:01 Lock	Locked,Unlock 09 min...	
<input type="checkbox"/>	30	192.200.17.200	/Default ...	192.200.17.200	None	2013-8-7 10:25:14 Lock	Locked,Unlock 09 min...	

Unlocking Online Users

The procedure for unlocking a user is as follows:

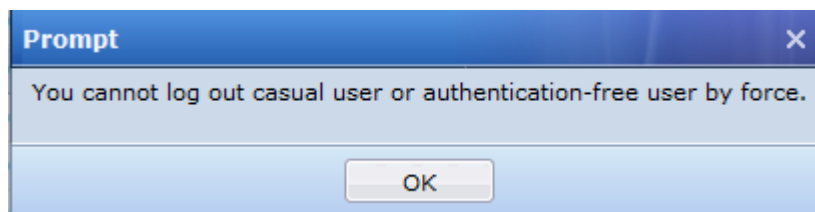
Select a locked user.

<input type="checkbox"/>	29	192.200.17.231	/Default ...	192.200.17.231	None	2013-8-7 10:25:01 Lock	Locked,Unlock 09 min...	
<input type="checkbox"/>	30	192.200.17.200	/Default ...	192.200.17.200	None	2013-8-7 10:25:14 Lock	Locked,Unlock 09 min...	

Click **Unlock** or the icon in the **Operation** column.

Forcibly Logging Out Online Users

The administrator can forcibly log out online users, excluding temporary users and those that do not require authentication. If the administrator attempts to forcibly log out a temporary user or a user that does not require authentication, the prompt shown in the figure below is displayed.

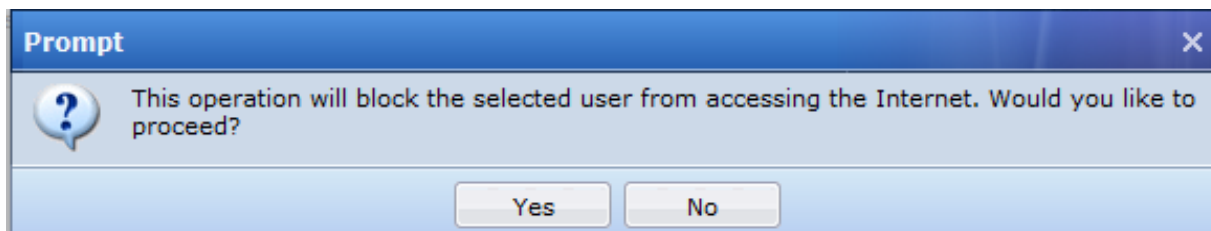


Password-authenticated users and single sign-on (SSO) users can be forcibly logged out. The procedure is as follows:

Select a user.

Users								
<input type="checkbox"/>	No.	Name(Display Name)	Group	IP Address	Authentication	Time Logged In/Locked	Online Duration	Operation
<input type="checkbox"/>	1	sangfor	/	192.200.17.10	Password based auth...	2013-8-7 10:28:28 Log In	40 seconds	

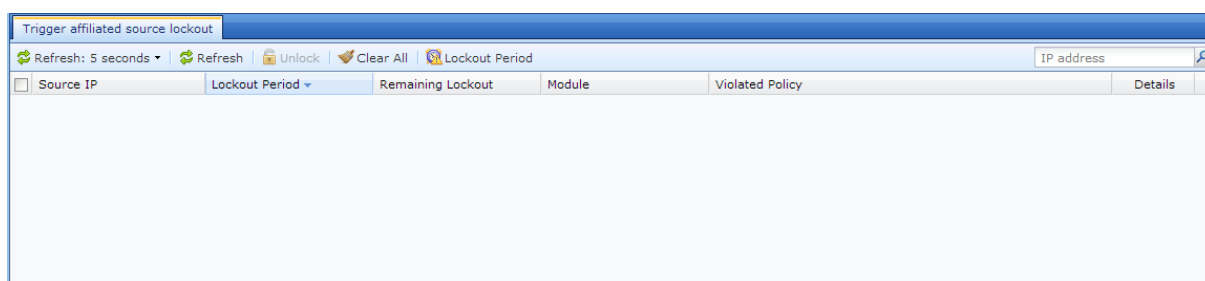
Click the **human icon** under Operation column. The prompt shown in the figure below is displayed.



Click **Yes** to log out the user.

Affiliated Source Lockout

The **Triggered affiliated source lockout** page displays the locked source IP addresses and the security policy that triggers the lockout propagation, when lockout propagation is enabled between the IPS rule and the data leak protection module, and between the Web application protection rule and the risk isolation module. See the figure below.




Click **Refresh: 5 seconds** to set the refresh interval.

Click **Refresh** to refresh the information immediately.

Select an item and click  to unlock the IP address.

Click  to clear all source IP addresses, thereby restoring the access permission of all IP addresses.

Click  to set the lockout period. For a source IP address that triggers the security policy, the default lockout period is 10 minutes. That is, this source IP address will be automatically unlocked in 10 minutes. You can set a longer lockout period.

You can search by IP address in the search text box.

Network

Interfaces

The **Interfaces** page displays information about the network interfaces and zones. The displayed information includes the physical interface, sub-interface, VLAN interface, zone, and link state propagation. See the figure below.

Name	Interface...	WAN ...	Ping	Type	Zone	IP Assignment	IP Address	Link Mode	MTU	Link State	Status
eth0	Manage i...	No	Allow	Route(layer 3)	None	Static IP	10.251.251.251/24	Full-duplex 1... Auto-negotia...	1500	Not detected...	✓
eth1		No	Deny	Route(layer 3)	WAN	Static IP	192.200.17.23/255.2...	Auto-negotia...	1500	Not detected...	✗
eth2		No	---	Bridge(layer...	LAN	Access access:1	--	Full-duplex 1... Auto-negotia...	1500	---	✓
eth3		Yes	---	Bridge(layer...	WAN_TEST	Access access:1	--	Full-duplex 1... Auto-negotia...	1500	---	✓

Physical Interface

The **Physical Interface** tab page displays the interface name, description, WAN, interface type, connection type, zone, IP address, dial-up status, MTU, operating mode, ping function, interface status, and link status. See the figure below.

Name	Interface...	WAN ...	Ping	Type	Zone	IP Assignment	IP Address	Link Mode	MTU	Link State	Status
eth0	Manage i...	No	Allow	Route(layer 3)	None	Static IP	10.251.251.251/24	Full-duplex 1... Auto-negotia...	1500	Not detected...	✓
eth1		No	Deny	Route(layer 3)	WAN	Static IP	192.200.17.23/255.2...	Auto-negotia...	1500	Not detected...	✗
eth2		No	---	Bridge(layer...	LAN	Access access:1	--	Full-duplex 1... Auto-negotia...	1500	---	✓
eth3		Yes	---	Bridge(layer...	WAN_TEST	Access access:1	--	Full-duplex 1... Auto-negotia...	1500	---	✓

Name: name of the network interface. The name of a physical interface cannot be changed.

Description: description of the network interface.

Type: type of the network interface. There are four interface types: route, transparent, virtual wire and bridge.

IP Assignment: IP address obtaining mode, including asymmetric digital subscriber line (ADSL), static IP address, and DHCP.

Zone: security zone to which the network interface belongs.


IP Address: IP address configured for the network interface. This column is left blank if no IP address is configured.

Dial-up status: When

Link Mode: operating mode of the network interface, such as auto-negotiation.

Ping: whether the network interface can be pinged.

Interface Status: link status of the network interface.  indicates that the network interface is connected,

whereas  indicates that no cable is connected to the network interface or the network interface fails.

Link State: link fault status of the network interface. The equipment can detect the link status through ping detection or DNS detection.

Status: whether the network interface is enabled.  Indicates that the network interface is enabled.

You can click an interface name, such as **eth0**, to open the interface editing page. See the figure below.

Edit Physical Interface

☒ Enable

Name: eth0

Description: Manage interface

Type: Route(layer 3)

Added To Zone: Select zone

Basic Attributes: ☐ WAN attribute ☒ Pingable

IPv4 IPv6

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 10.251.251.251/24

Next-Hop IP:

Line Bandwidth

Outbound: 8 Mbps

Inbound: 8 Mbps

OK Cancel

Type specifies the interface type. It defines the data forwarding function of the equipment. There are four interface types.

Route: An IP address need to be configured for a route interface, which provides the routing and forwarding function.

Transparent: A transparent interface equals a common switching interface. No IP address needs to be configured for a transparent interface, which does not support routing or forwarding. Data is forwarded based on the MAC address table.

Virtual wire: A virtual wire interface is also a common switching interface. No IP address needs to be configured for a virtual wire interface, which does not support routing or forwarding. Data is directly forwarded through the interface that is paired with the virtual wire.

Bridge: A bridge interface is connected to a switch with the mirroring function and is used to mirror data that passes through the switch.

NGAF 5.2 does support IPv6 addressing. You can click **IPv6** tab to configure IPv6 IP address for the interface. See the figure below.

Edit Physical Interface

☒ Enable

Name: eth0

Description: Manage interface

Type: Route(layer 3)

Added To Zone: Select zone

Basic Attributes: ☐ WAN attribute ☒ Pingable

IPv4 IPv6

IP Assignment: ☒ Static ☐ DHCP

Static IP: 2001::1/64

Next-Hop IP:

Line Bandwidth

Outbound: 8 Mbps

Inbound: 8 Mbps

OK Cancel

For details about the configuration description of these interface types, see section 5.1.



1. The ETH0 is a route interface. You cannot change the interface type.
2. You can add a management IP address for the ETH0 interface. The default management IP address 10.251.251.251/24 cannot be deleted.
3. The IP address of any interface cannot be on the 1.1.1.0/24 network segment.

Sub-Interface

The **Sub-Interface** tab page displays whether a physical interface is a route interface and the scenario where VLAN trunk needs to be enabled for the route interface. See the figure below.

Name	Zone	IP Assignment	IP Address	MTU	Ping	Link State	Delete

Name: name of the sub-interface. The interface name is generated automatically and cannot be changed. For example, the name of a sub-interface on VLAN2 of the eth0 interface is generated as eth0.2.

Description: description of the sub-interface.

Zone: zone to which the sub-interface belongs.

IP Address: IP address of the sub-interface.

MTU: MTU value of the sub-interface.

Ping: whether the sub-interface can be pinged.

Link State: whether link detection is enabled for the sub-interface.

For details about the configuration procedure of a sub-interface, see section 5.1.4.



The IP address of any interface cannot be on the 1.1.1.0/24 network segment.

VLAN Interface

The **VLAN Interface** tab page displays the VLAN list of the equipment. See the figure below.

Interfaces								
Physical Interface Sub-Interface VLAN Interface Aggregate Interface Zone Link State Propagation								
+ Add X Delete Refresh								
<input type="checkbox"/>	Name	Zone	IP Assignment	IP Address	MTU	Ping	Link State	Delete
<input type="checkbox"/>	veth.1	WAN	Static	192.200.17.24/24	1500	Allow	Not detected yet	X

Click **Add** to add a VLAN interface, as shown in the figure below.

Name: specifies the VLAN ID. Enter the ID of the VLAN to which the equipment is added.

Basic Attributes: specifies whether the VLAN interface can be pinged.

IP Assignment: can be set to **Static** or **DHCP**. If it is set to **Static**, enter the IP address on the corresponding VLAN network segment.

The method of setting **Link State Detection** and **Advanced** is the same as that of setting the route interface.



The IP address of any interface cannot be on the 1.1.1.0/24 network segment.

Aggregate Interface

The **Aggregate Interface** tab page displays the aggregated interface list of the equipment. See the figure below.

Interfaces

Physical InterfaceSub-InterfaceVLAN InterfaceAggregate InterfaceZoneLink State Propagation

+ AddX DeleteRefresh

<input type="checkbox"/>	Name	WAN Attrib...	Ping	Type	Zone	Link Mode	IP Address	MTU	Physical Interfa...	Delete
--------------------------	------	---------------	------	------	------	-----------	------------	-----	---------------------	--------

Click **Add** to add an aggregated interface, as shown in the figure below.

Add Aggregate Interface

Name: aggr. (1~4) ⓘ

Description:

Type: Route(layer 3) ▼

Added To Zone: Select zone ▼

Work Mode: Active-standby ▼

Basic Attributes: ☐ WAN attribute ☒ Pingable

Static IP: Type here ⓘ

Next-Hop IP: ⓘ

Member Interfaces

Available: eth1, eth2, eth3

Selected:

Add ▶

◀ Delete

Line Bandwidth

Outbound: 1024 Mbps ▼

Inbound: 1024 Mbps ▼

Advanced

Specify MTU and MAC address. Settings

OK Cancel

Name: specifies the name of the aggregated interface.

Description: specifies the description of the aggregated interface.

Type: specifies the interface type. Three types are supported: route, bridge and virtual wire.

Added To Zone: specifies the zone to which the aggregated interface belongs.

Work Mode: specifies the work mode supported by the aggregated interface. It can be set to load balancing-hash, load balancing-RR, or active-standby.

Basic Attributes: The method of setting basic attributes is the same as that of setting the route interface.

Member Interfaces: specifies the interfaces to be aggregated.

The method of setting **Link State Detection** and **Advanced** is the same as that of setting the route interface.

Zone

The **Zone** tab page displays the zone to which an interface belongs, so as to provide modules for invoking, including the content security, traffic management, and firewall modules. There are three types: layer 2, layer 3 and virtual line. The layer 2 zone supports all transparent interfaces, the layer 3 zone supports all route interfaces, and the virtual wire zone supports all virtual wire interfaces. See the figure below.

Zone Name	Forward Mode	Interfaces	Device Mgt Privilege	Allowed Address	Delete
WAN	Route(layer 3)	eth1,veth.1	WebUI	All	In use
LAN	Bridge(layer 2)	eth2			In use
WAN_TEST	Bridge(layer 2)	eth3			In use

Click **Add**. The page for adding a zone is displayed as follows:

Add Zone

Name:

Forward Mode:

- ☒ Bridge(layer 2)
- ☐ Route(layer 3)
- ☐ Virtual wire(layer 1)

Interface

Available:

Selected:

Add ▶

◀ Delete

Device Mgt Privilege

- ☒ Web UI
- ☐ SSH
- ☒ SNMP

Allowed IP Address:


OK Cancel

Name: specifies the name of the zone.

Forward Mode: specifies the type of the zone. If it is set to **Bridge (layer 2)**, the transparent interfaces not belonging to any zone are displayed in the interface list. If it is set to **Route (layer 3)**, the route interfaces including both sub-interfaces and VLAN interfaces not belonging to any zone are displayed in the interface list. If it is set to **Virtual wire (layer 1)**, the virtual wire interfaces not belonging to any zone are displayed in the interface list.

Interface: specifies the interfaces to be added to the zone. You can click **Add** or **Delete** to add or delete interfaces.

Device Mgt Privilege: specifies whether to allow login from this zone. You can choose to log in to the equipment in Web UI, SSH, or SNMP mode and then manage the equipment. See the figure below.

Allowed IP address: specifies the source IP address for logging in to the equipment. Click  to select and add IP groups.

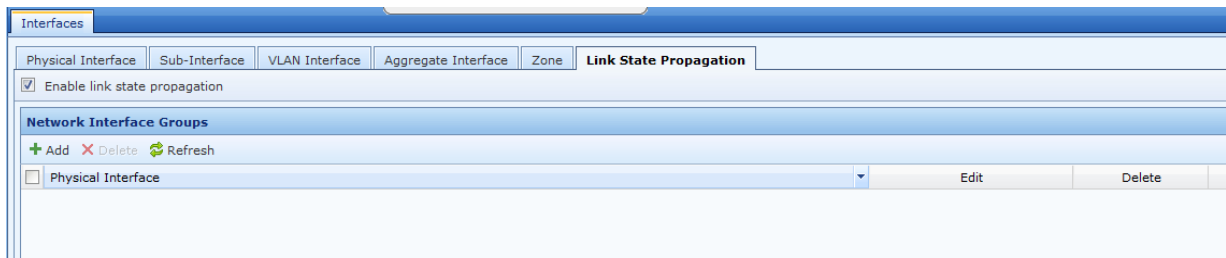
Click **OK**.



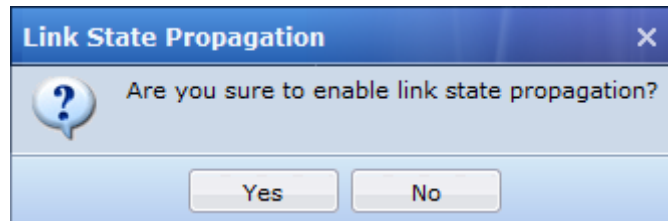
1. An interface can belong only to one zone. A zone can contain multiple interfaces.
2. A zone can contain both LAN interfaces and VLAN interfaces.

Link State Propagation

The **Link State Propagation** tab page allows you to add the inbound and outbound data forwarding interfaces to the same propagation group when the NGAF equipment operates in load balancing mode. This ensures that all interfaces in the same propagation group are consistent in the state. For example, if the network cable is disconnected from an interface in a propagation group, all other interfaces in the group become unavailable automatically. After the network cable is connected to this interface again and electric signals resume, all other interfaces in the group also resume, ensuring load balancing. See the figure below.

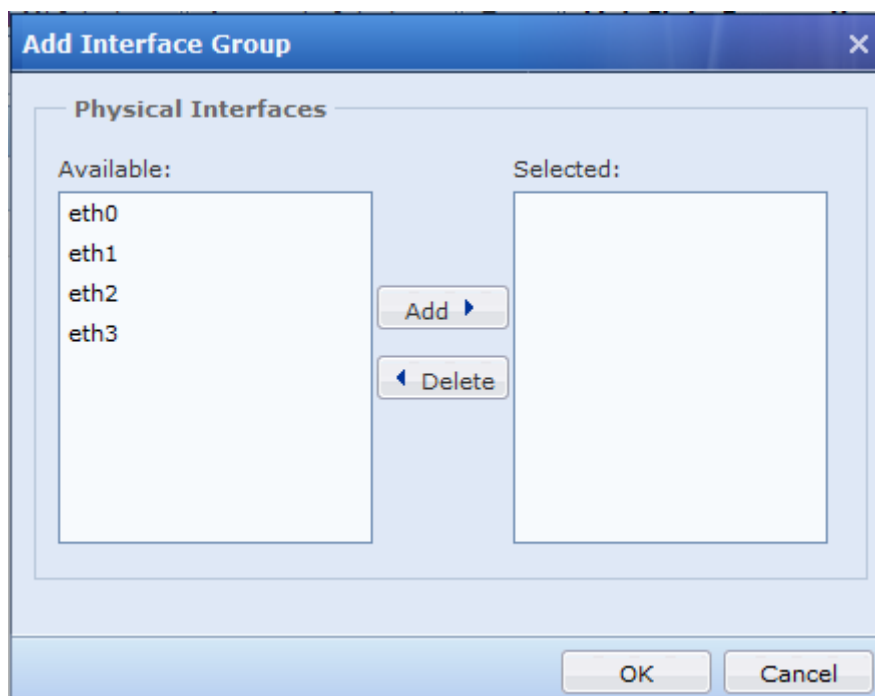


Enable link state propagation is the main switch for enabling link state propagation. After it is selected, the following screen will appear:



Click **Yes** to enable link state propagation.

Click **Add** to add an interface propagation group.



Name: specifies the name of the interface propagation group.

Physical Interfaces: specifies interfaces to be added to the propagation group. Only physical interfaces are supported. A propagation group can contain multiple interfaces. You can click **Add** or **Delete** to add or delete interfaces.

Click **OK** to save the settings.



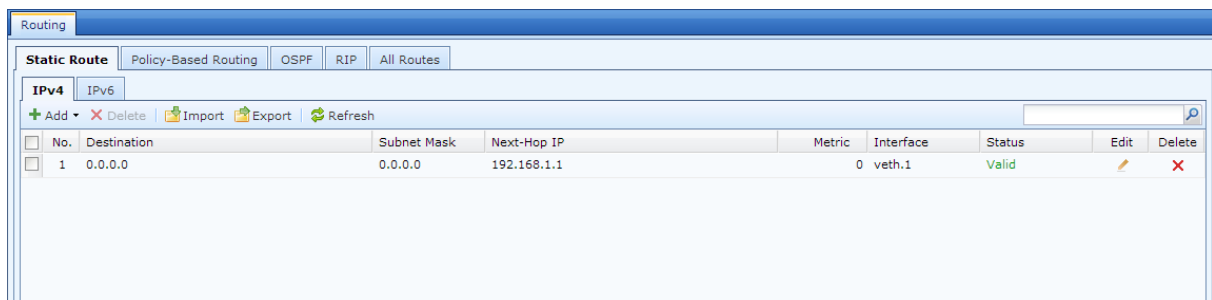
If the IP address of an interface is set to be in the format of IP/mask-HA, this interface cannot be added to a propagation group.

Routing

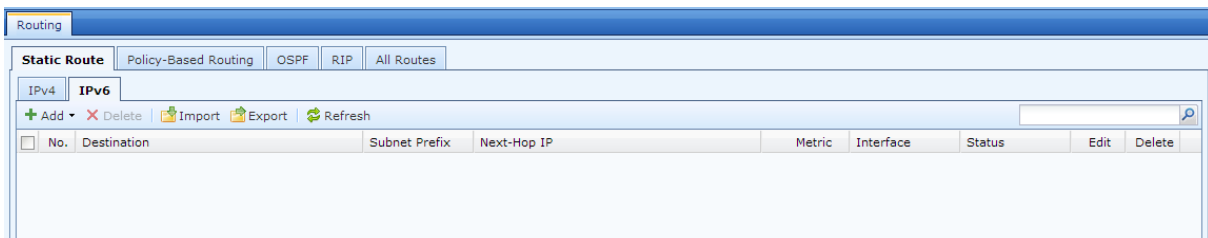
The **Routing** page contains the **Static Route**, **Policy-Based Routing**, **OSPF**, **RIP**, and **All Routes** tab pages. When the equipment needs to communicate with IP addresses on different network segments, data forwarding needs to be implemented through routing.

Static Route

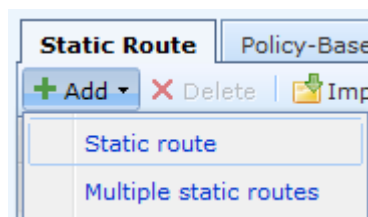
In the navigation area, choose **Network** > **Routing** and access the **Static Route** tab page. In NGAF 5.2, Static Route supports both IPv4 and IPv6 addresses. **IPv4** is shown in the figure below:



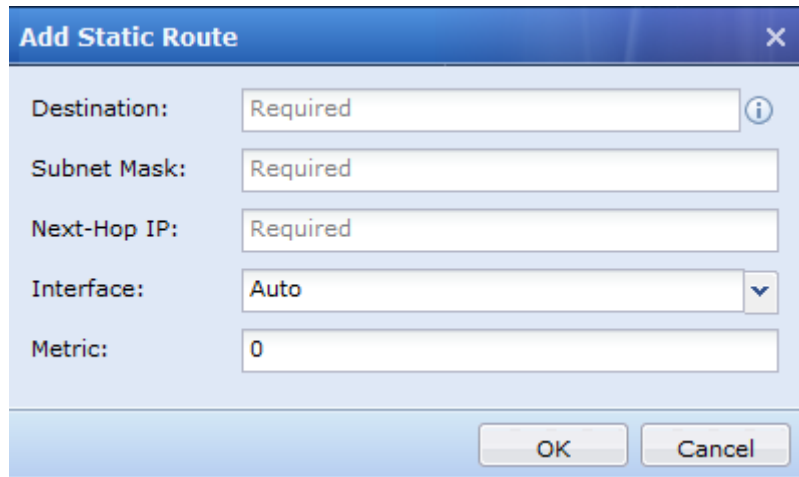
Click on **IPv6** tab for configuration in IPv6 environment.



Click **Add** to open the **Static Route** page. You can choose to add a single or multiple static routes.



The page for adding a single static route is as follows:



The 'Add Static Route' dialog box contains the following fields:

- Destination:** Required
- Subnet Mask:** Required
- Next-Hop IP:** Required
- Interface:** Auto
- Metric:** 0

Buttons: OK, Cancel

Destination: destination network ID.

Subnet Mask: subnet mask of the target network.

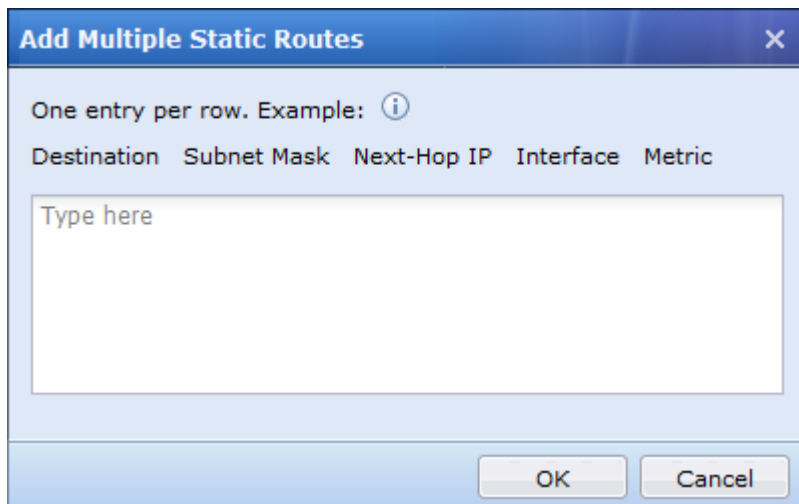
Next-Hop IP: next-hop IP address to the target network.

Interface: interface through which data is forwarded.

Metric: metric of the static route.

Click **OK** to save the settings.

The page for adding multiple static routes is as follows:



The 'Add Multiple Static Routes' dialog box contains the following elements:

- One entry per row. Example: ⓘ
- Table headers: Destination, Subnet Mask, Next-Hop IP, Interface, Metric
- Text area: Type here

Buttons: OK, Cancel

Enter the destination IP address, subnet mask, next-hop IP address, interface, and metric in sequence. A line indicates a static route.

Click **OK** to save the settings.

Click **Advanced Search** to search for route entries based on specified conditions.



It is recommended that Interface be set to Auto for a static route. If multiple interface IP addresses of the equipment are on the same network segment, manually specify the interface of the static route.

Policy-Based Routing

The **Policy-Based Routing** tab page allows you to select inbound and outbound lines based on the source/destination IP address, source/destination port, and protocol when multiple external interfaces of the equipment are connected to multiple external lines. This ensures that different data is forwarded through different external lines.

In the navigation area, choose **Network > Routing** and access the **Policy-Based Routing** tab page.



Policy-based routing is required in the following scenarios:

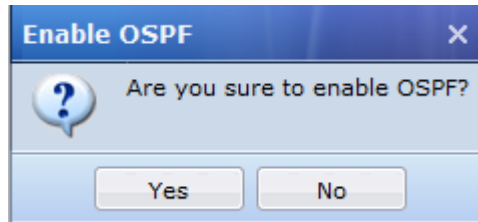
1. The interface or next hop is selected based on the source IP address or protocol. Data flows of internal users accessing the public network are distributed. That is, internal users on different network segments access the public network through different line interfaces. When there are multiple external lines, internal users are directed to different links to access applications such as online bank and online payment. These applications have high security requirements. Therefore, some servers need to authenticate the source IP addresses. If an internal user accesses such an application multiple times by using different source IP addresses, the server ends the access connection. In this case, the policy-based routing function enables internal users to access these applications from a specific interface or next hop. This ensures that a fixed source IP address is used to access these applications.
2. There are multiple external lines on the equipment. The optimal line is used in preference based on policy-based routing, bandwidth ratio and weighted minimum traffic. In this way, lines are selected dynamically, thereby implementing effective use of line bandwidth and load balancing.

OSPF

The **OSPF** tab page allows you to enable OSPF for the NGAF equipment and set the OSPF dynamic routing protocol. This tab page covers four modules: **Network Segments**, **Interfaces**, **Parameters**, and **Status**. See the figure below.



Select the **Enable OSPF** check box to enable OSPF for the equipment. The prompt shown in the figure below is displayed.



Click **Yes** to save the setting.

When the NGAF equipment is in an area not adjacent to the backbone OSPF area, you need to enable and configure a virtual connection. Click **Add Virtual Connection**. The page shown in the figure below is displayed.

A configuration window titled "Add Virtual Connection" with a close button (X) in the top right corner. It features a checkbox labeled "Enable". Below this are input fields for "Area ID:" and "Router ID:". A section titled "Timer" contains four input fields: "Hello Time:", "Retransmit Interval:", "Delay:", and "Dead Time:". Below the timer section are radio buttons for "Encryption:" with options "Plaintext", "MD5", and "None" (selected). At the bottom is a "Password:" input field. The window concludes with "OK" and "Cancel" buttons.

Click **Enable** to configure a virtual connection.

Area ID: ID of the backbone area.

Router ID: ID of the peer router in the virtual connection.

Timer: Set the transmission interval, retransmission interval, transmission delay, and expiration interval of Hello packets, in seconds.

Hello Time: interval for retransmitting Hello packets. The default value is **10** seconds.

Retransmit Interval: interval for retransmitting connection status packets adjacent to the interface. The default value is **10** seconds.

Delay: delay in transmitting a link status update packet. The default value is **5** seconds.

Dead Time: expiration time of Hello packets. If no Hello packet is received within the specified expiration time,

the OSPF neighbor is considered unreachable. The value of **Dead Time** is usually 4 times that of **Hello Time**. The default value is **40** seconds.

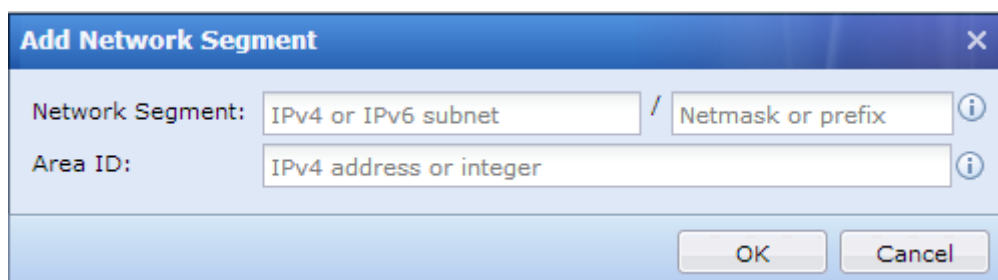
Encryption: encryption mode of packets. It can be set to **Plaintext**, **MD5** or **None**.

Password: password for encrypting packets.

Click **OK** to save the settings.

3.2.2.3.1 Network Segments

The **Network Segments** page allows you to set the network segment to be published. Click **Add**. The page shown in the figure below is displayed.



The 'Add Network Segment' dialog box has a title bar with a close button. It contains two input fields: 'Network Segment' with a placeholder 'IPv4 or IPv6 subnet / Netmask or prefix' and 'Area ID' with a placeholder 'IPv4 address or integer'. Both fields have information icons to their right. At the bottom right are 'OK' and 'Cancel' buttons.

Network Segment: specifies the address of the network segment to be published. The format is IP address(IPv4 or IPv6)/mask.

Area ID: specifies the area for which the network segment is bound. Usually it is the ID of the backbone area.

3.2.2.3.2 Interfaces

The **Interfaces** page displays information about the interface corresponding to the network segment published in **Network Segments**. Suppose that the network segment shown in the figure below is added in **Network Segments**.

Network Segments		
+ Add - Delete		
No.	Network Segment	Area ID
1	192.200.19.0/24	0.0.0.0

The automatically generated interface configurations are shown in the figure below.

Interfaces						
Name	IP Address	Passive Interface	Authentication	Neighbor Age	Election Priority	Retransmit Interval
eth1	192.200.19.18/24	No	None	40	1	5

Click **Name**. The page shown in the figure below is displayed.

Name:	eth1
Interface IP:	192.200.19.18/24
Passive Interface:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Authentication:	<input type="radio"/> Plaintext <input type="radio"/> MD5 <input checked="" type="radio"/> None
Password:	
Cost:	1
Neighbor Age(sec):	40
Msg Delivery Interval(sec):	10
Election Priority:	1
Retransmit Interval(sec):	5
Enable DD packet MTU detection:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Name: name of the interface corresponding to the network segment published in **Network Segments**.

IP: IP address of the interface.

Passive Interface: an interface that does not send OSPF link status. After an interface is configured as a passive interface, a direct route can be published. However, the OSPF packets of the interface are blocked and no neighbor relationship can be established. The default value is **No**.

Encryption: encryption mode of packets. It can be set to **Plaintext**, **MD5** or **None**. The default value is **Plaintext**.

Password: password for encrypting packets when **Encryption** is set to **Plaintext** or **MD5**.

Cost: cost for sending packets through a link. The cost affects the metric of the link state advertisement (LSA), which directly affects the OSPF path selection result. The value range is 1-65535. The default value is **1**.

Aging Time (s): expiration time. The default value is 40 seconds.

Transmit Interval (s): interval for transmitting Hello packets. The default value is **10** seconds.

Election Priority: priority value of a router. A router with the priority value 0 will not be elected as the designated router (DR) or backup designated router (BDR). The DR is elected from the routers on the same network segment by exchanging Hello packets. A router includes the elected DR in a Hello packet and sends the packet to other routers on the same network segment. If two routers on the same network segment elect themselves as the DR, the router with the higher priority prevails. If they share the same priority, the router with the larger ID prevails. The default value is **1**.

Retransmit Interval (s): interval for retransmitting LSAs. By default, the interval for retransmitting LSAs between adjacent routes is 5 seconds.

Enable MTU Un-match Detection: OSPF-enabled routers describe their link state databases (LSDBs) by using DD packets during database synchronization. By default, no MTU value is filled in DD packets. That is, the MTU value is 0.

3.2.2.3.3 Parameters

Choose **OSPF > Parameters**. The page shown in the figure below is displayed.

Router ID: 108.250.70.76

Intra-Area Priority: 10

Inter-Area Priority: 110

External Priority: 150

SPF Interval: 5

Route Re-Advertisement

Re-advertise Direct Route: ☐ Yes ☒ No
Metric:

Re-advertise RIP Route: ☐ Yes ☒ No
Metric:

Re-advertise Static Route: ☐ Yes ☒ No
Metric:

Re-advertise Default Route: ☐ Yes ☒ No

Default Metric: 10

OK Restore to Defaults

Router ID: router ID of the NGAF equipment.

Intra-Area Priority: priority carried in an intra-area LSA after it is calculated and output to the routing table. This priority is called administration distance (AD) on Cisco equipment. The default value is **10**.

Inter-Area Priority: priority carried in an inter-area LSA after it is calculated and output to the routing table. The default value is **110**.

External Priority: priority assigned to an external route to be output to the routing table after shortest path first (SPF) calculation. The default value is **150**.

SPF Interval: interval for SPF calculation. If the LSDB changes, the shortest path needs to be recalculated. The default value is **5** seconds.

Route Re-Advertisement: indicates whether to introduce direct routes, RIP routes, and static routes as external route information to the OSPF routing table. You can set the metric value of an introduced route.

Re-advertise Direct Route: indicates whether to introduce direct routes as external routing information to the OSPF routing table. You can set the metric value of an introduced route. The default metric value is **10**.

Re-advertise RIP Route: indicates whether to introduce RIP routes as external routing information to the OSPF routing table. You can set the metric value of an introduced route. The default metric value is **20**.

Re-advertise Static Route: indicates whether to introduce static routes as external routing information to the OSPF routing table. You can set the metric value of an introduced route. The default metric value is **20**.

Default Metric: default number of hops of an introduced route. If no metric value is specified when a route is introduced, the default metric value takes effect. That is, the number of hops of this introduced route is 10. The default value is **10**.

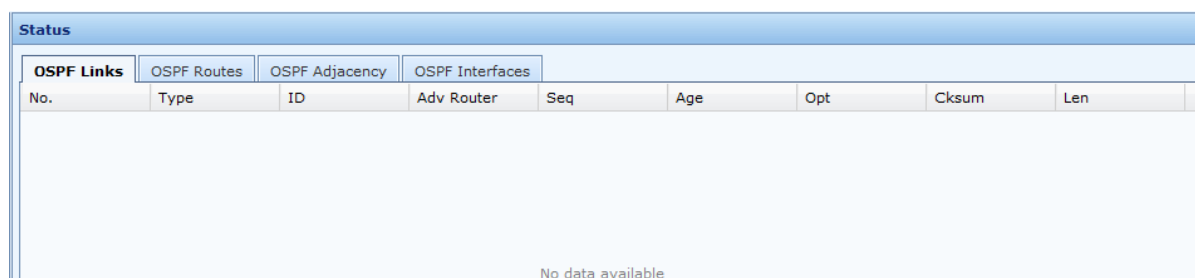
Click **OK** to save and apply the settings.

3.2.2.3.4 Status

The **Status** page allows you to view OSPF links, OSPF routes, OSPF adjacencies, and OSPF interfaces.

3.2.2.3.4.1 OSPF Links

The **OSPF Links** tab page is shown below.



No.	Type	ID	Adv Router	Seq	Age	Opt	Cksum	Len
No data available								

Type: LSA type.

ID: ID of the router to which the LSA belongs. The asterisk (*) indicates an LSA generated by a router itself.

Adv Router: router that advertises the LSA.

Seq: sequence number of the LSA.

Age: time that the LSA has been received. The LSA is aged after the expiration time elapses.

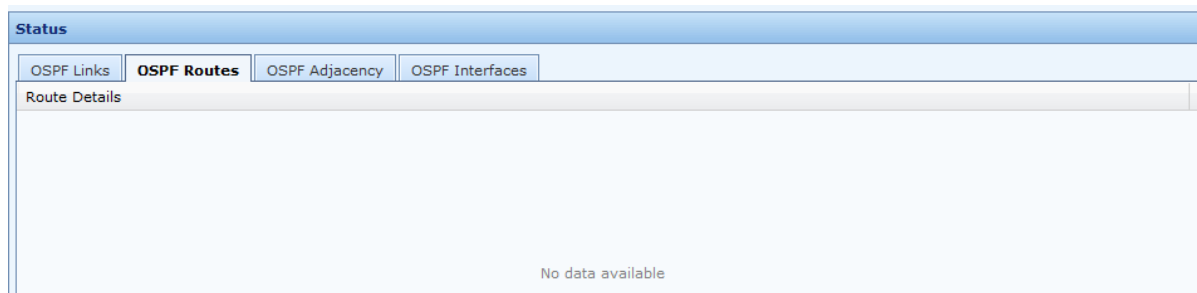
Opt: option information carried in Hello packets. A router can reject messages sent from a neighbor that shares the same option filed with this router.

Cksum: checksum of the LSA.

Len: length of the LSA.

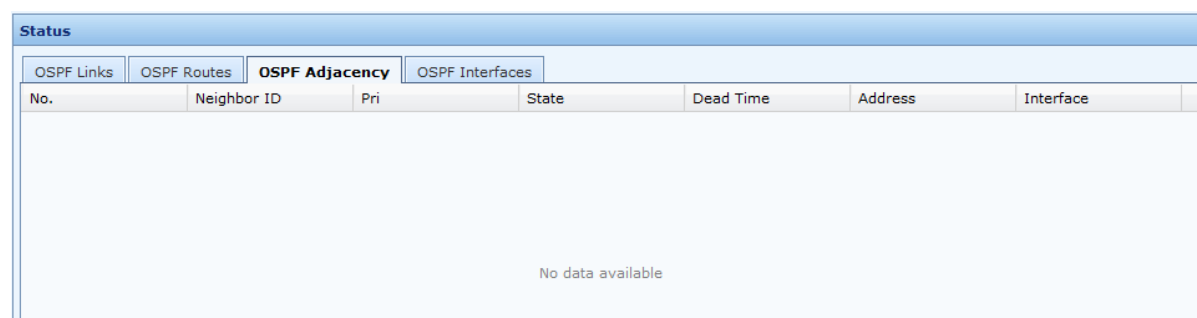
3.2.2.3.4.2 OSPF Routes

The **OSPF Routes** tab page displays OSPF routes. See the figure below.



3.2.2.3.4.3 OSPF Adjacency

The **OSPF Adjacency** tab page is shown below.



Neighbor ID: ID of the neighboring router.

Pri: priority of the neighboring router.

State: functional status of the neighboring router.

Dead Time: expiration time of the router. If the neighbor does not send a Hello packet, the router enters the DEAD state after the specified time elapses.

Address: IP address of the interface of the neighbor connected to the router. When OSPF packets are transmitted to the neighbor, the value of **Address** is the next-hot IP address. OSPF_VL1 is a virtual connection identifier.

Interface: interface of the neighbor connected to the router.

3.2.2.3.4.4 OSPF Interfaces

The **OSPF Interfaces** tab page is shown below.

Status						
OSPF Links OSPF Routes OSPF Adjacency OSPF Interfaces						
Interface	IP	Area	State	DR	BDR	

Interface: interface name.

IP: IP address of the interface.

Area: area to which the interface belongs.

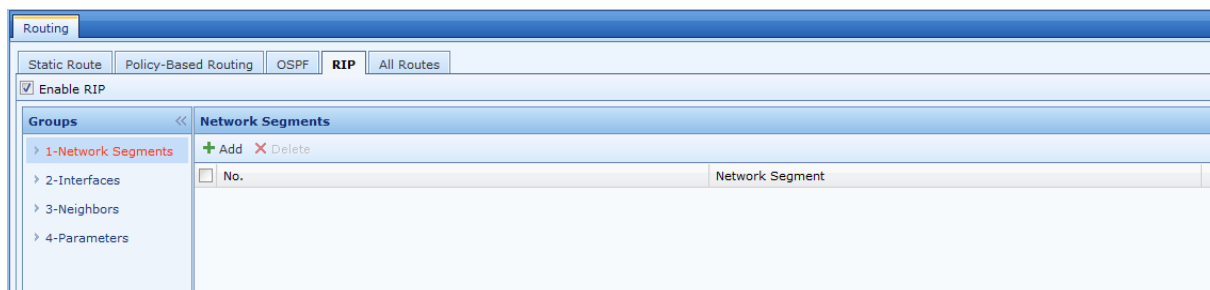
State: role of the interface.

DR: IP address of the DR in the area.

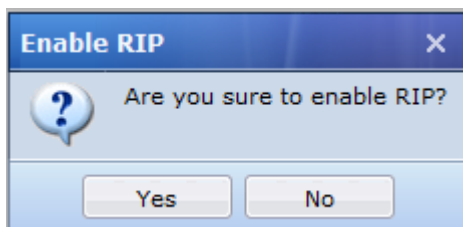
BDR: IP address of the BDR in the area.

RIP

The **RIP** tab page allows you to enable RIP for the NGAF equipment and set the RIP dynamic routing protocol. This tab page covers four modules: **Network Segments**, **Interfaces**, **Neighbors**, and **Parameters**. See the figure below.



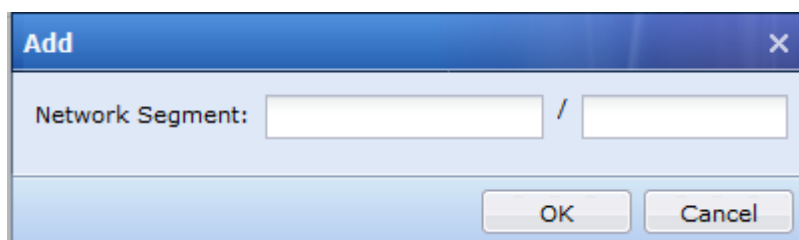
Select the **Enable RIP** check box to enable RIP for the equipment. The prompt shown in the figure below is displayed.



Click **Yes** to save the setting.

3.2.2.4.1 Network Segments

The **Network Segments** page allows you to set the network segment of an interface to RIP network segment. Click **Add**. The page shown in the figure below is displayed.



The 'Add' dialog box has a title bar with 'Add' and a close button. It contains a 'Network Segment' label followed by two text input fields separated by a forward slash. At the bottom are 'OK' and 'Cancel' buttons.

Network Segment: specifies the address of the network segment to be published. The format is IP address/mask.

Click **OK** to save and apply the settings.

3.2.2.4.2 Interfaces

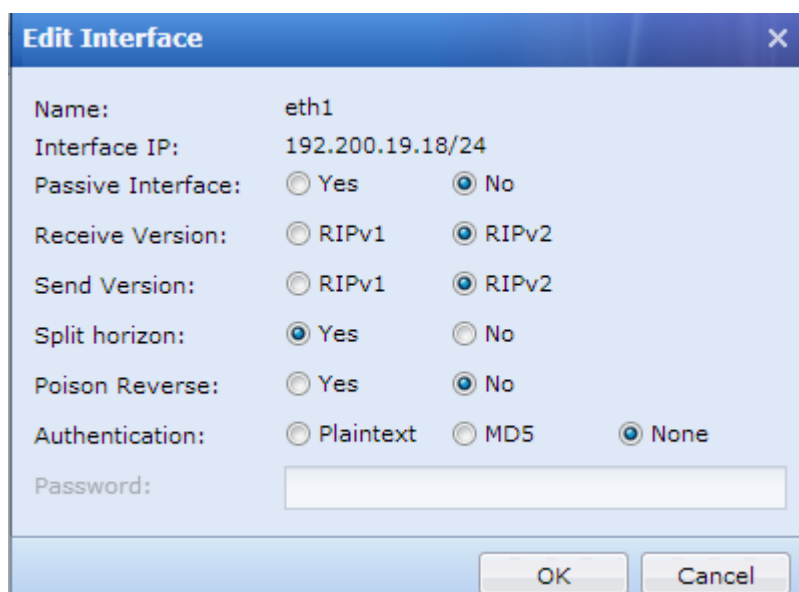
The **Interfaces** page displays information about the interfaces corresponding to the network segment published in **Network Segments**. The interfaces can receive and send RIP packets. Suppose that the network segment shown in the figure below is added in **Network Segments**.

Network Segments	
+ Add - Delete	
No.	Network Segment
<input type="checkbox"/> 1	192.200.19.0/24

The automatically generated interface configurations are shown in the figure below.

Interfaces			
<input checked="" type="checkbox"/> Name	IP Address	Passive Interface	Authentication
<input checked="" type="checkbox"/> eth1	192.200.19.18/24	No	None

Click **Name**. The page shown in the figure below is displayed.



The 'Edit Interface' dialog box has a title bar with 'Edit Interface' and a close button. It contains the following fields and options:

- Name: eth1
- Interface IP: 192.200.19.18/24
- Passive Interface: ☐ Yes ☒ No
- Receive Version: ☐ RIPv1 ☒ RIPv2
- Send Version: ☐ RIPv1 ☒ RIPv2
- Split horizon: ☒ Yes ☐ No
- Poison Reverse: ☐ Yes ☒ No
- Authentication: ☐ Plaintext ☐ MD5 ☒ None
- Password: (empty text field)

At the bottom are 'OK' and 'Cancel' buttons.

Name: name of the interface corresponding to the network segment published in **Network Segments**.

Interface IP Address: IP address of the interface.

Passive Interface: RIP work status on the interface. The default value is **No**.

Version (receive): version of RIP packets received on the interface. If the version is set to **RIPv2**, both **RIPv1** and **RIPv2** packets can be received.

Version (send): version of RIP packets sent on the interface. **RIPv1** packets are transmitted in broadcast mode. **RIPv2** packets are transmitted in broadcast or multicast mode. By default, **RIPv2** packets are transmitted in multicast mode. If the version is set to **RIPv2**, both **RIPv1** and **RIPv2** packets can be sent.

Level Division: whether to allow level division. Level division indicates that a route learned from an interface cannot be sent through this interface. Level division can avoid routing loops. By default, level division is allowed.

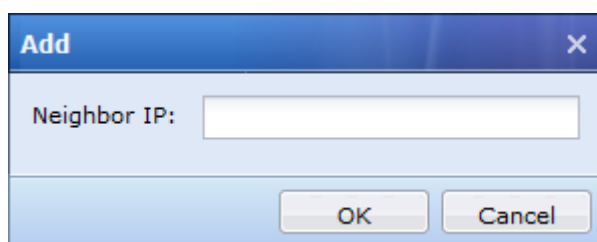
Reversion: whether to allow reversion. After reversion is enabled, a route received from an interface will be flooded through this interface. The metric of this route is infinite. By default, reversion is disabled.

Encryption: mode for encrypting packets. It can be set to **Plaintext**, **MD5** or **None**. **RIPv1** does not support packet encryption. **RIPv2** supports plaintext and MD5 encryption.

Password: password for encrypting packets when **Encryption** is set to **Plaintext** or **MD5**.

3.2.2.4.3 Neighbors

The **Neighbors** page allows you to set the IP address of a neighboring router that runs RIP. See the figure below.



Click **OK** to save the settings.

3.2.2.4.4 Parameters

Choose **RIP > Parameters**. The page shown in the figure below is displayed.

RIP Parameters

Route Priority: ⓘ

Timers

Update Timer: ⓘ

Timeout Timer: ⓘ

Flush Timer: ⓘ

Route Re-Advertisement

Re-advertise Direct Route: ☐ Yes
Metric: ⓘ

☒ No

Re-advertise OSPF Route: ☐ Yes
Metric: ⓘ

☒ No

Re-advertise Static Route: ☐ Yes
Metric: ⓘ

☒ No

Default Metric: ⓘ

OK Restore to Defaults

RIP Parameters: You can set the route priority and timer in the **RIP Parameters** panel.

Route Priority: RIP priority. The optimal route is selected among the routes that are obtained through the routing protocol determined by the priority. The larger the priority value is, the lower the priority is. You can manually configure the RIP priority. The default RIP priority value is **120**.

Update Timer: interval for periodically updating routes. The default value is **30** seconds.

Timeout Timer: timeout time of a route. If the information about this route is not received within the specified time, the number of hops of this route is set to 16, which means that this route is unreachable. The default value is **180** seconds.

Flush Timer: time of advertising unreachable routes. Before the flush timer expires, RIP continues to advertise unreachable routes. If the flush timer expires, the unreachable routes are deleted from the routing table.

Route Re-Advertisement: You can configure other routes such as direct routes, OSPF routes, and static routes to be introduced to RIP, and set the metric values of introduced routes in the **Route Re-Advertisement** pane.

Re-advertise Direct Route: indicates whether to introduce direct routes as external routing information to the RIP routing table. You can set the metric value of an introduced route. The default metric value is **10**.

Re-advertise OSPF Route: indicates whether to introduce OSPF routes as external routing information to the RIP

routing table. You can set the metric value of an introduced route. The default metric value is **20**.

Re-advertise Static Route: indicates whether to introduce static routes as external routing information to the RIP routing table. You can set the metric value of an introduced route. The default metric value is **20**.

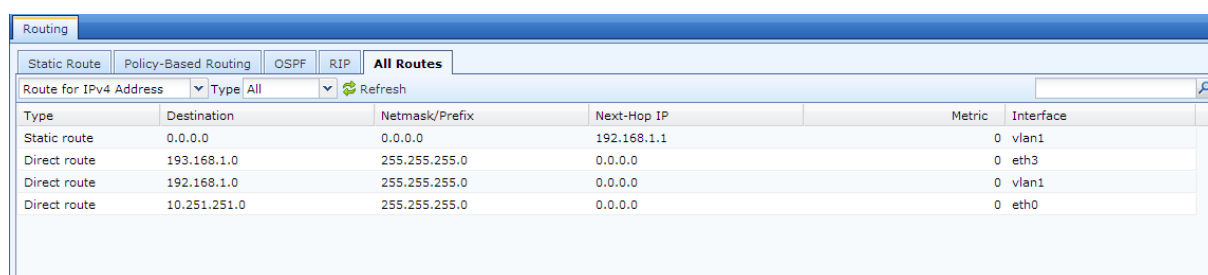
Default Metric: default number of hops of an introduced route. If you do not specify the metric value of an introduced route, the default metric value takes effect. The default metric value is **10**.

Click **OK** to save and apply the settings.


Click **Restore to Defaults** to restore the default parameter values.

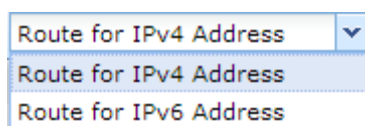
All Routes

The **All Routes** tab page displays all routes on the equipment, including direct routes, static routes and those learned through a dynamic routing protocol. See the figure below.

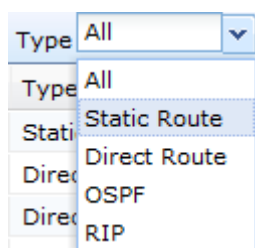



Type	Destination	Netmask/Prefix	Next-Hop IP	Metric	Interface
Static route	0.0.0.0	0.0.0.0	192.168.1.1	0	vlan1
Direct route	193.168.1.0	255.255.255.0	0.0.0.0	0	eth3
Direct route	192.168.1.0	255.255.255.0	0.0.0.0	0	vlan1
Direct route	10.251.251.0	255.255.255.0	0.0.0.0	0	eth0

Route for IPv4 and IPv6 address selection is available. Click  to select the Internet Protocol choices. Refer to figure below:



Click  next to **Type** to filter routes by type. See the figure below.



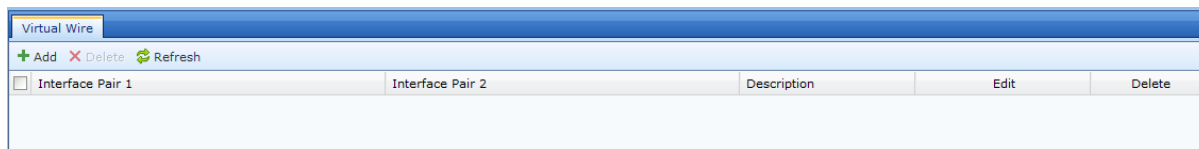
Click  to refresh the route entries to be displayed.

Virtual Wire

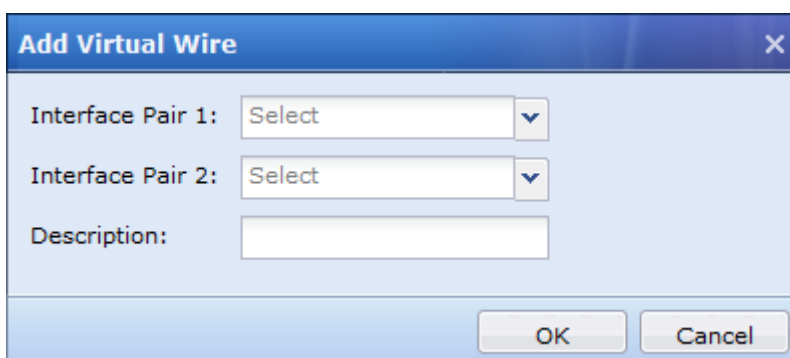
The virtual wire function involves setting a physical interface group on the NGAF equipment. For example, set interfaces A and B to form a virtual wire group. After packets are forwarded to the equipment through interface A,

all other data is forwarded through interface B, except the data whose destination IP address is that of the NGAF equipment. That is, the other data is directly forwarded without searching the layer 2 MAC address table and layer 3 routing check. However, the data is still controlled by all types of security policies. The virtual wire function helps improve the data forwarding efficiency on the NGAF equipment and avoid data forwarding errors caused by a disordered MAC address table.

The **Virtual Wire** page is shown below.



Click **Add** to add a virtual wire. See the figure below.



Description: Enter the name and description of the virtual wire to be added.

Interface Pair 1: Select a physical interface with the virtual interface attribute.

Interface Pair 2: Select a physical interface with the virtual interface attribute.

Click **OK** to save and apply the settings.



Only virtual interfaces can form virtual wire groups. Virtual interfaces and virtual wire groups must be configured at the same time.

Advanced Options

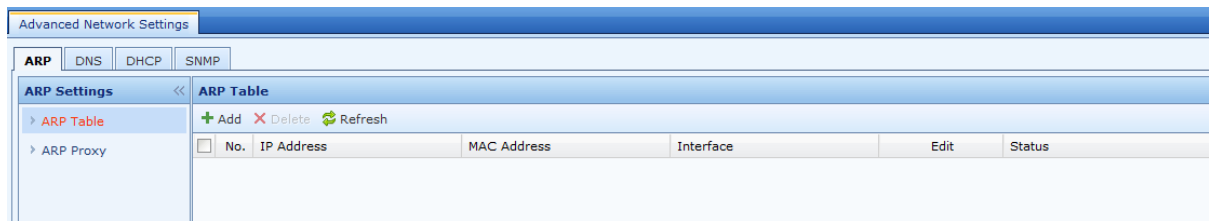
The **Advanced Options** page includes the **ARP**, **DNS**, **DHCP** and **SNMP** tab pages.

ARP

There are two menus in the navigation area of the **ARP Settings** pane, that is, **ARP Table** and **ARP Proxy**.

3.2.4.1.1 ARP Table

You can bind static IP/MAC entries in the **ARP Table** pane. See the figure below.



Click **Add** to add a static ARP entry. See the figure below.

The 'Add ARP Entry' dialog box contains three input fields: 'IP Address:', 'MAC Address:', and 'Interface:'. The 'Interface' field is a dropdown menu currently set to 'Auto'. There is a 'Get MAC Address' button next to the 'MAC Address' field. At the bottom right are 'OK' and 'Cancel' buttons.

IP Address: IP address to which a static ARP entry is to be bound.

MAC Address: MAC address to which the static ARP entry is to be bound.

Interface: Set it to an interface on the same network segment as the bound IP address.

3.2.4.1.2 ARP Proxy

The ARP proxy function indicates that the NGAF equipment proxy responds to ARP requests to protect hosts on the internal network. See the figure below.

The 'Add ARP Proxy' dialog box contains three input fields: 'Start IP:', 'End IP:', and 'Interface:'. The 'Interface' field is a dropdown menu. At the bottom right are 'OK' and 'Cancel' buttons.

For details about the configuration description of the ARP proxy, see section 5.3.

DNS

On the **DNS** tab page, you can set the DNS proxy function and the DNS server for the NGAF equipment to access the public network. See the figure below.

The screenshot shows the 'Advanced Network Settings' window with the 'DNS' tab selected. It contains two main sections: 'DNS Server' and 'DNS Proxy'. In the 'DNS Server' section, 'Preferred DNS' is set to '8.8.8.8' and 'Alternate DNS' is set to '202.188.1.133'. The 'DNS Proxy' section includes a descriptive text and two radio buttons: 'Enable' (which is unselected) and 'Disable' (which is selected). An 'OK' button is located at the bottom right of the window.

You can set the DNS servers for the NGAF equipment to access the public network in **Preferred DNS** and **Alternate DNS**.

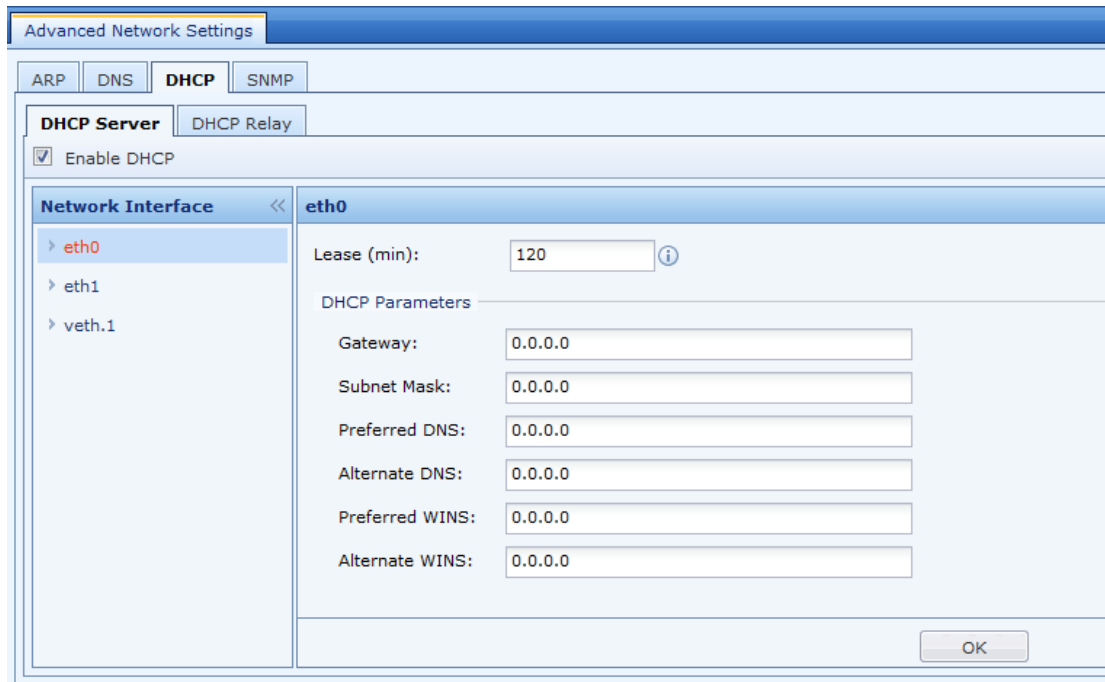
DNS Proxy: It can be set to **Enable** or **Disable**. After the DNS proxy function is enabled, the DNS of internal users is set to the IP address of an interface of the NGAF equipment. The proxy responds to the DNS requests of internal users and forwards the requests to the preferred and alternate DNS servers.

DHCP

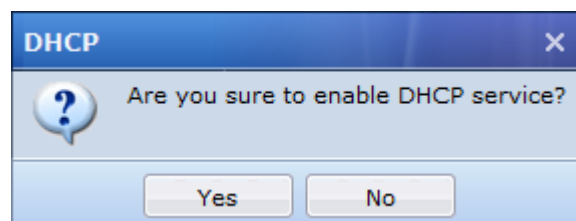
On the DHCP tab page, you can set the NGAF equipment as a DHCP server or DHCP relay. NGAF 5.2 DHCP server does not support IPv6.

3.2.4.3.1 DHCP Server

The **DHCP Server** tab page is shown below.



Select **Enable DHCP**. The prompt shown in the figure below is displayed.



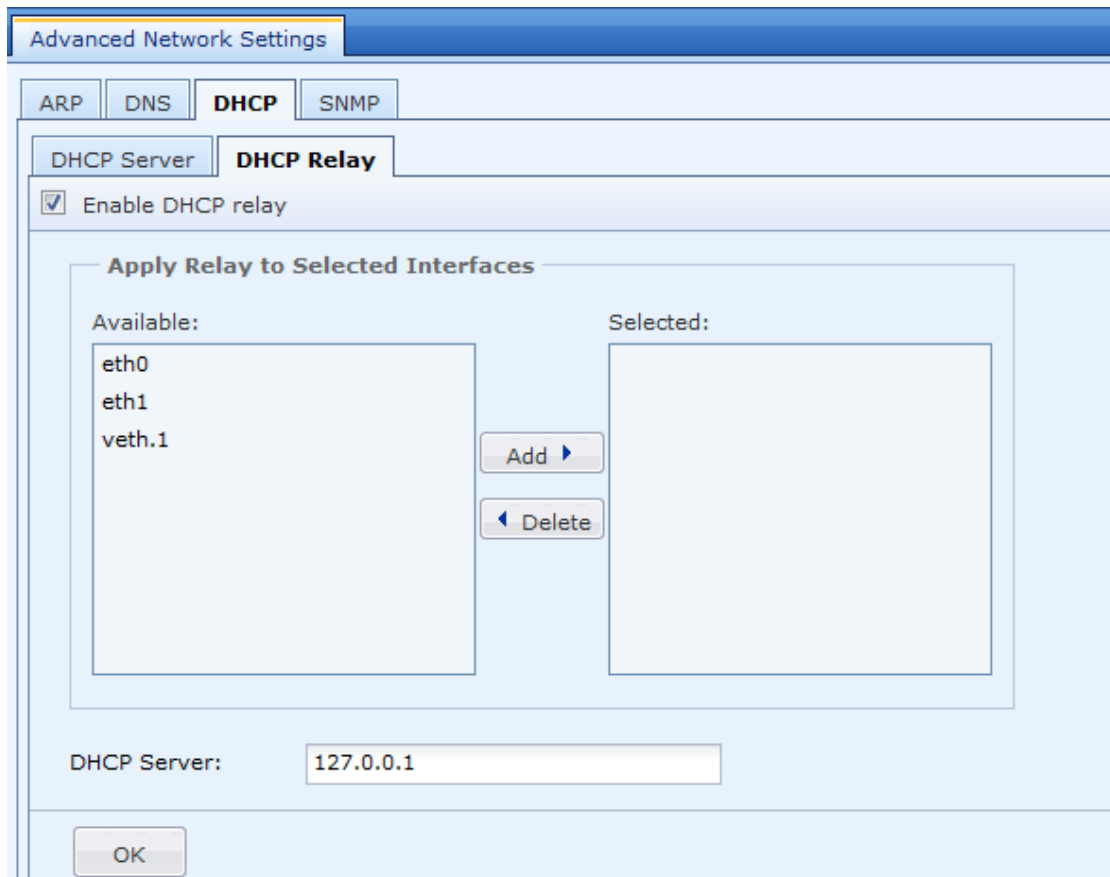
Click **Yes** to enable the DHCP service.

The **Network Interface** pane displays all route interfaces, sub-interfaces and VLAN interfaces on the equipment. You can assign IP addresses through these interfaces.

For details about the configuration description of the DHCP server, see section 5.4.1.

3.2.4.3.2 DHCP Relay

The DHCP relay function applies when the IP addresses of the DHCP server and DHCP client are on different IP network segments. See the figure below.

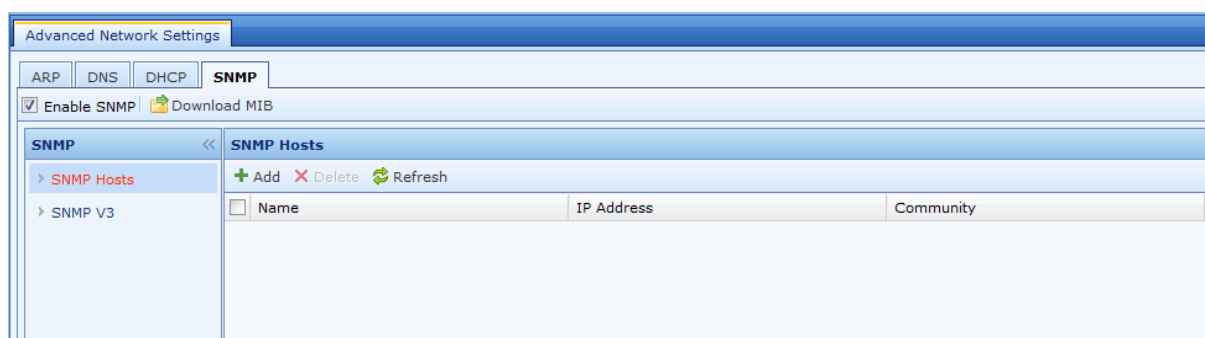


For details about the configuration description of the DHCP relay, see section 5.4.2.

SNMP

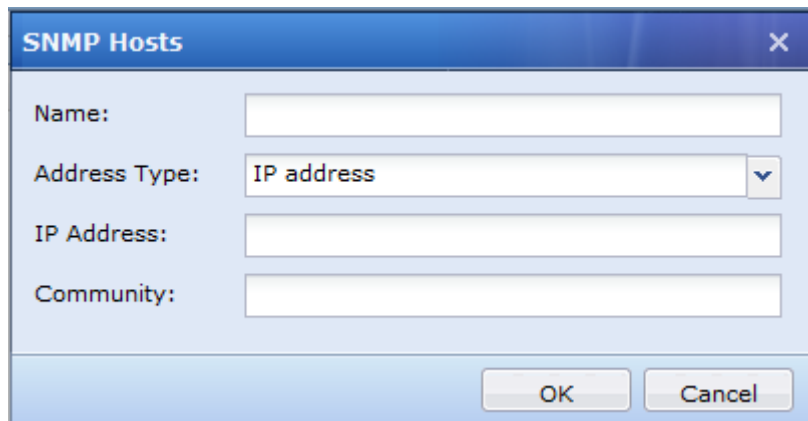
SNMP allows other network management devices or software to manage and view information about SANGFOR equipment in through SNMP. The information includes interface status, traffic and routes. This facilitates centralized management, maintenance and monitoring of the network.

In the navigation area, choose **Network** > **Advanced Network Settings** and access the **SNMP** tab page.



Select **Enable SNMP**. Then other devices and management software can access information about SANGFOR equipment through SNMP.

In the **SNMP Hosts** pane, you can set other devices to connect to the NGAF equipment through SNMPv2, as well as connection parameters. Click **Add** to add a management host. See the figure below.



The **SNMP Hosts** dialog box contains the following fields:

- Name:** A text input field for the host name.
- Address Type:** A dropdown menu currently set to **IP address**.
- IP Address:** A text input field for the IP address or range.
- Community:** A text input field for the community name.

At the bottom right are **OK** and **Cancel** buttons.

Name: name of the management host.

Address Type: type of the management host. It can be set to **IP address** or **Subnet**. If it is set to **IP address**, the SNMP manager is a host. If it is set to **Subnet**, the SNMP manager is a subnet and all hosts on this subnet can manage the NGAF equipment through SNMP.

IP Address: IP address or IP address range of the SNMP manager. If the SNMP manager is a host, set **IP Address** to the IP address of the SNMP host. If the SNMP manager is a subnet, set **IP Address** to the subnet address and mask of the SNMP subnet.

Community: community name used by the SNMP host to access the NGAF equipment.

Click **OK** to save the settings.

In the **SNMP V3** pane, you can set advanced parameters when SNMPv3 is used as the communication protocol. See the figure below.



The **SNMP V3** dialog box contains the following fields:

- Context:** A text input field with an information icon (i).
- Authentication Password:** A text input field with an information icon (i).
- Confirm Password:** A text input field.
- Encryption Password:** A text input field with an information icon (i).
- Confirm Password:** A text input field.
- Security:** A dropdown menu currently set to **Encrypted**.

At the bottom right are **OK** and **Cancel** buttons.

Context: name of the SNMPv3 user.

Authentication Password: password used by the SNMPv3 user for authentication. The password must be a string of eight characters without spaces. It is encrypted by using the MD5 algorithm.

Encryption Password: password for encrypting packets. The password must be a string of eight characters without spaces. It is encrypted by using the Data Encryption Standard (DES) algorithm.

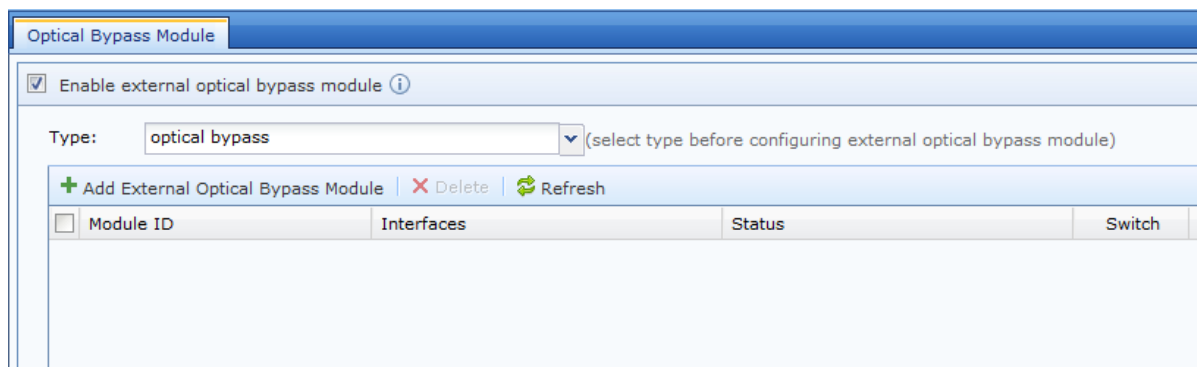
Security: whether to encrypt SNMP authentication and management information. It can be set to **Encrypted** or

None. If encryption is enabled, both encryption and authentication are performed. That is, data is encrypted first and then message digest calculation is performed. If encryption is disabled, only authentication is performed.

Click **OK** to save the settings.

Optical Bypass Module

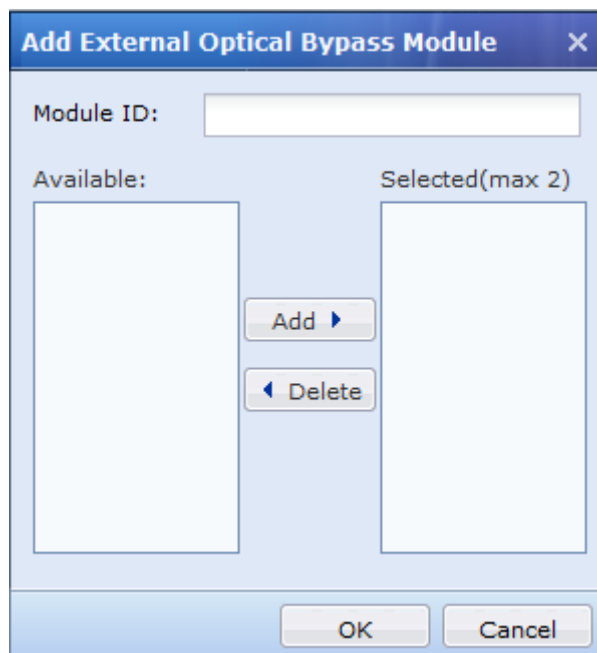
The optical bypass function is supported. The configuration page is shown below.



The screenshot shows the 'Optical Bypass Module' configuration window. It has a title bar with the text 'Optical Bypass Module'. Below the title bar, there is a checkbox labeled 'Enable external optical bypass module' with an information icon. Below this, there is a 'Type:' label followed by a dropdown menu showing 'optical bypass' and a hint '(select type before configuring external optical bypass module)'. Below the dropdown, there are three buttons: '+ Add External Optical Bypass Module', 'X Delete', and 'Refresh'. Below these buttons is a table with four columns: 'Module ID', 'Interfaces', 'Status', and 'Switch'. The table is currently empty.

Type: Only optical bypass is supported. Note that optical bypass and two-node hot backup are mutually exclusive.

Add External Optical Bypass Module: Select the corresponding optical module interface and configure it.



The screenshot shows the 'Add External Optical Bypass Module' dialog box. It has a title bar with the text 'Add External Optical Bypass Module' and a close button. Below the title bar, there is a 'Module ID:' label followed by a text input field. Below this, there are two labels: 'Available:' and 'Selected(max 2)'. Below 'Available:' is a large empty rectangular box. Below 'Selected(max 2)' is a large empty rectangular box. Between these two boxes are two buttons: 'Add' with a right arrow and 'Delete' with a left arrow. At the bottom of the dialog box are two buttons: 'OK' and 'Cancel'.

Security Databases

Vulnerability Database

The vulnerability database contains characteristics of attack packets that perform attacks based on system and program vulnerabilities. When passing through the equipment, these packets can be blocked based on the settings to protect the server. See the figure below.



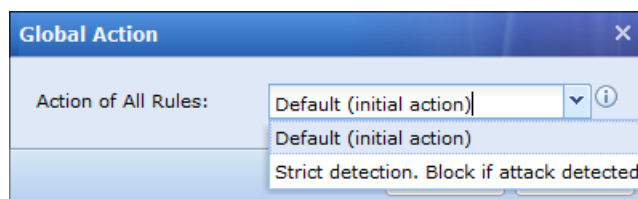
Vulnerability ID	Vulnerability Name	Type	Threat Level	Action
12030557	Polycom RealPresence Resource Manager Absolute path disclosure Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030555	Polycom RealPresence Resource Manager Arbitrary file upload Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030549	Novell ZenWorks Configuration Management 11.3.1 Traversal And Code Execution Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030548	PHPMoAdmin 1.1.2 Remote Code Execution Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030546	IBM Tivoli Endpoint Manager HTML Injection Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030545	Persistent Systems Radia Client Automation Remote Code Execution Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030544	Lexmark MarkVision Enterprise Arbitrary File Upload Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030543	ManageOwage Series Products Unauthenticated File Upload Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030542	Lotus Mail Encryption Server Local File Inclusion Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030541	Tuleap Enalean Remote PHP Code Injection Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030540	MantisBT SQL Injection Vulnerability	Application Vulnerability	High	Enable. Block if attack detected
12030539	ManageEngine EventLog Analyzer Information Disclosure Vulnerability	Application Vulnerability	Medium	Enable. Allow if attack detected

Enable Cloud-based analysis engine: After the cloud-based analysis engine is enabled, suspicious unrecognized traffic is automatically uploaded to the SANGFOR cloud server. The traffic is analyzed, identified, and matched with existing attack traffic modes on the cloud server, thereby determining whether the traffic aims to perform attacks.

Click **Global Action** to unify all modified IPS Vulnerability Rules.

If **Default (initial action)** is selected, the system will reset all IPS Vulnerability Rules actions to default.

If **Strict detection. Block if attack detected** is selected, all the actions will become “Enabled. Block if attack detected.” regarding any of the threat level. In default option, Medium level threats will be **allowed**. After enabled this option, all Medium level threats will be **blocked**.



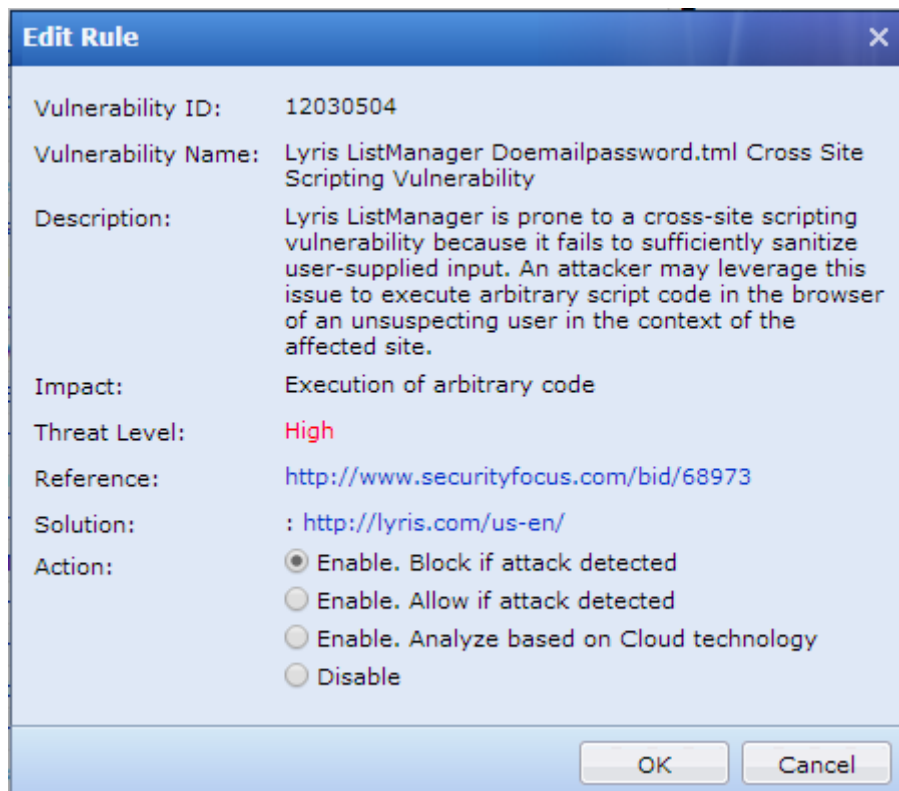
The **Vulnerability ID** column lists the IDs of existing vulnerabilities. You can search for vulnerabilities by ID. When the server is blocked according to an IPS rule, you can view the vulnerability ID in the data center. After finding the vulnerability ID, you can choose to ignore this rule.

The **Vulnerability Name** column lists the names of vulnerabilities.

The **Type** column lists the types of existing vulnerabilities, such as backdoor.

The **Threat Level** column lists the levels of vulnerabilities. There are three levels: high, medium and low.

The **Action** column lists the actions taken by the equipment when attacks are performed. There are four actions: **Enable. Block if attack detected**, **Enable. Log event if attack detected**, **Enable. Analyze based on Cloud technology**, and **Disable**. You can define actions. Click a vulnerability name to open the editing page. See the figure below.



The 'Edit Rule' dialog box displays the following information:

- Vulnerability ID:** 12030504
- Vulnerability Name:** Lyris ListManager Doemailpassword.tml Cross Site Scripting Vulnerability
- Description:** Lyris ListManager is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.
- Impact:** Execution of arbitrary code
- Threat Level:** High
- Reference:** <http://www.securityfocus.com/bid/68973>
- Solution:** : <http://lyris.com/us-en/>
- Action:**
 - ☒ Enable. Block if attack detected
 - ☐ Enable. Allow if attack detected
 - ☐ Enable. Analyze based on Cloud technology
 - ☐ Disable

Buttons: OK, Cancel

Enable. Block if attack detected: The current rule is enabled. In case of an attack based on this vulnerability, corresponding packets are blocked.

Enable, Log event if attack detected: The current rule is enabled. In case of an attack based on this vulnerability, the attack is logged and the packets are not blocked.

Enable. Analyze based on Cloud technology: If this option is selected, the equipment performs analysis and detection by using the cloud technology.

Disable: The current rule is disabled. The equipment does not detect this vulnerability.




1. The Action attribute is set for the vulnerability database before delivery. When you need to modify a rule, edit it.
2. You can edit only one rule of the vulnerability database at a time.

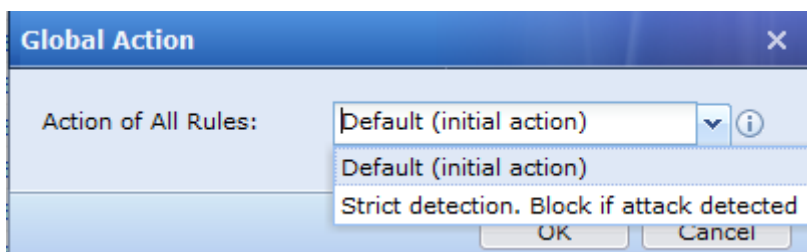
WAF Signature Database


The WAF signature database contains characteristics of application-layer attack packets that perform attacks based on structured query language (SQL) injection, cross-site scripting (XSS) attacks, and cross-site request forgery. When passing through the equipment, these packets can be blocked based on the settings to protect the server. See the figure below.

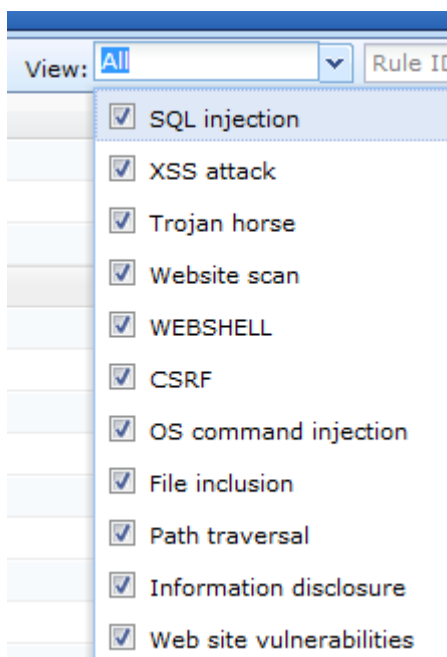
WAF Signature Database				
<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable <input type="checkbox"/> Enable Cloud-based analysis engine <input type="checkbox"/> Global Action <input type="checkbox"/> Restore Default Action				
		View: All		Rule ID or name
Rule ID	Rule Name	Type	Threat Level	Action
<input type="checkbox"/> 13120115	Mybb Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120114	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120113	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120112	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120111	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120110	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120109	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120108	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120107	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120106	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120105	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120104	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120103	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120102	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120101	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120100	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...
<input type="checkbox"/> 13120099	Wordpress Application Exploit Attack	Web site vulnerabilities	High	Enable. Block if attack de...

Click  to modify rules of the WAF signature database in a unified manner.

If **Default (initial action)** is selected, the default action takes effect. If **Strict detection. Block if attack detected** is selected, the action **Enable. Block if attack detected** takes effect for all rules. By default, the system allows all rules with the medium threat level. After strict detection is enabled, rules of all threat levels are blocked.



View specifies the rule database of the current protection type. Click  to view the rule ID based on the protection type. See the figure below.

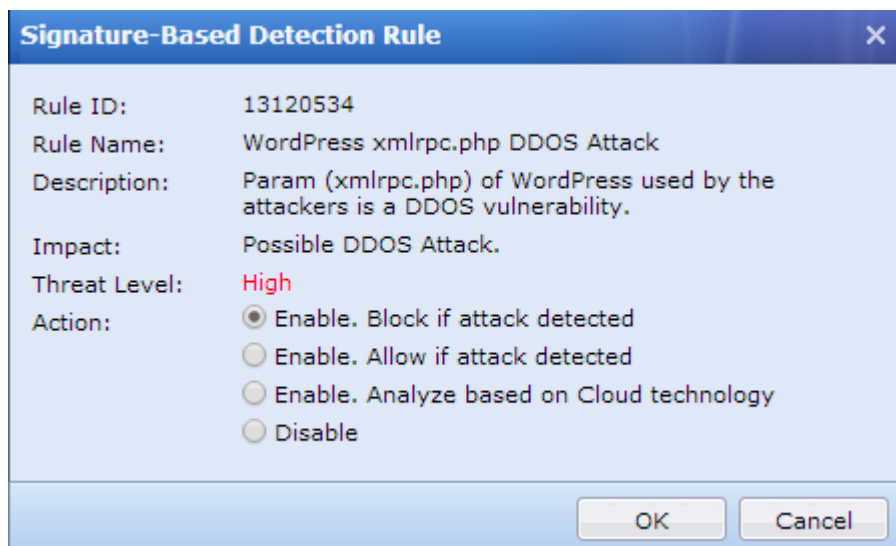


Rule Name: name of the protection rule.

Type: protection type of the current protection rule, such as SQL injection.

Threat Level: level of the vulnerability. There are three levels: high, medium and low.

Action: actions taken by the equipment when the attack is performed. There are four actions: **Enable. Block if attack detected**, **Enable. Log event if attack detected**, **Enable. Analyze based on Cloud technology**, and **Disable**. You can define actions. Click a vulnerability name to open the editing page. See the figure below.



Enable. Block if attack detected: The current rule is enabled. When the attack is detected, corresponding packets are blocked.

Enable. Log event if attack detected: The current rule is enabled. When the attack is detected, it is logged and the packets are not blocked.

Enable. Analyze based on Cloud technology: If this option is selected, the equipment performs analysis and detection by using the cloud technology.

Disable: The current rule is disabled. The equipment does not detect this rule.

Vulnerability Analysis Rules

The vulnerability analysis rules contains the rules of vulnerabilities that can be used for scanning and detection for servers and hosts. When the equipment runs RT vulnerability scanner to scan servers, the equipment will detect the vulnerabilities of the server if the rules match during scanning. The analysis will be logged and used to generate report for user.

Vulnerability Analysis Rule				
<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable		View: All		
Rule ID	Rule Name	Category	Threat Level	Action
<input type="checkbox"/> 15090282	JCMS 2010 Database Configuration Load Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090281	JCMS 2010 SQL Injection Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090280	JCMS 2010 Arbitrary File Upload Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090279	JCMS 2010 Local File Include Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090278	KingCMS5.0 Fckeditor Component Upload WebShell Vulnerability Detection	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090277	Joomla Zap Calendar Component XSS Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090276	Joomla Flexicontent Component Remote Code Execution Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090275	Joomla Explorer Component XSS Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090274	Joomla Multi Calendar Component XSS Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090273	Joomla 2.5 Remote Privilege Escalation Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090272	Joomla 3.2 SQL Injection Vulnerability Detection	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090271	Joomla 3.2 HTML Injection Vulnerability Detection	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090270	Joomla Simple File Lister Component Local File Inclusion Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090269	Joomla Jotloader Component Local File Inclusion Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090268	Joomla JoomTouch Component Local File Inclusion Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090267	Drupal v6 OpenID Module Authentication Bypass Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090266	Drupal v7 Access Control Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090265	Drupal v6 OpenID Module Authentication Bypass Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090264	Drupal v6 OpenID Module Authentication Bypass Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090263	Drupal v7 Security Bypass Vulnerability	Cms Vulnerability	High	Enable
<input type="checkbox"/> 15090262	Drupal v7 Information Disclosure Vulnerability	Cms Vulnerability	High	Enable

Rule Name: name of the protection rule.

Category: protection type of the current protection rule, such as Cms vulnerability.

Threat Level: level of the vulnerability. There are three levels: high, medium and low.

Action: actions taken by the equipment when the attack is performed. There are two actions: **Enable** and **Disable**. You can define actions. Click a vulnerability name to open the editing page. See the figure below.

Edit Rule

Rule ID:

15090282

Vulnerability Name:

JCMS 2010 Database Configuration Load Vulnerability

Description:

JCMS 2010 is vulnerable to a Database Configuration Load attack, because it fails to sanitize invalid content in url /jcms/workflow/design/readxml.jsp?flowcode=. An attacker may exploit this flaw to read database configuration.

Impact:

An attacker may use it to get sensitive information or get admin authority.

Threat Level:

High

Reference:

Solution:

Use web firewall.

Action:

☒ Enable
 ☐ Disable

OK

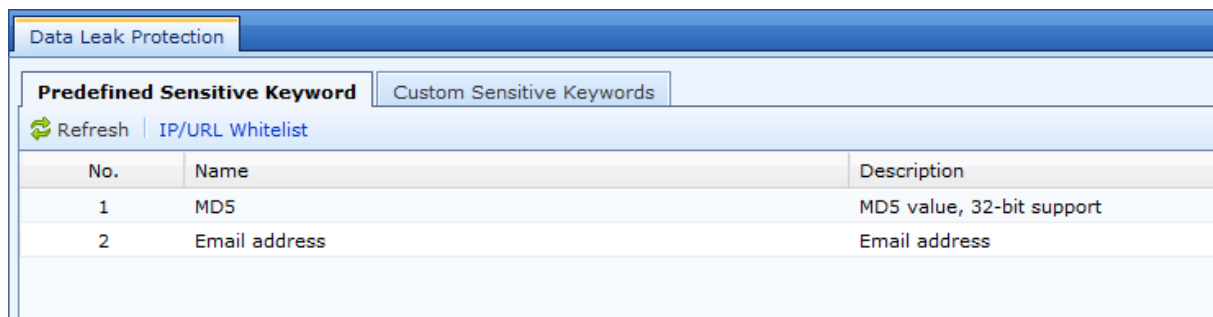
Cancel

Enable: The current rule is enabled, the equipment performs analysis and detection on servers based on the rule. When the vulnerability is detected, it is logged.

Disable: The current rule is disabled. The equipment does not detect this rule.

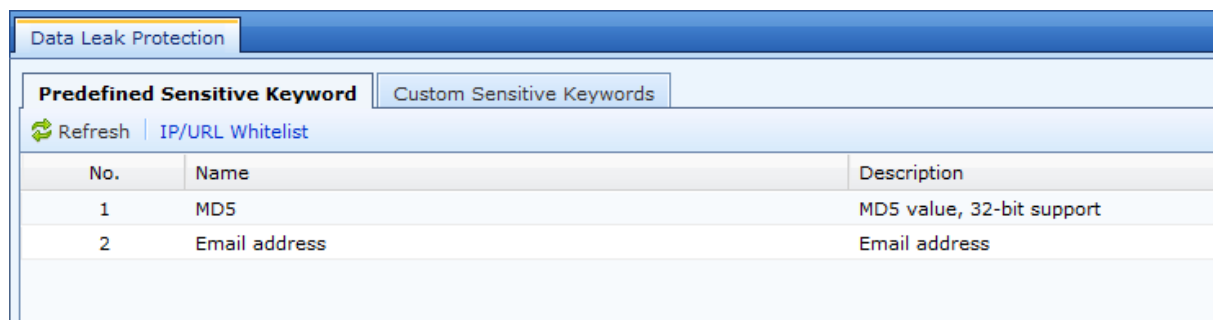
Data Leak Protection

The data leak protection database contains the regular expressions of some sensitive information, such as ID number, mobile phone number, and bank account. You can define the sensitive keywords. After data leak protection is enabled, the sensitive information is blocked by the equipment, preventing the sensitive information about users from being leaked. See the figure below.

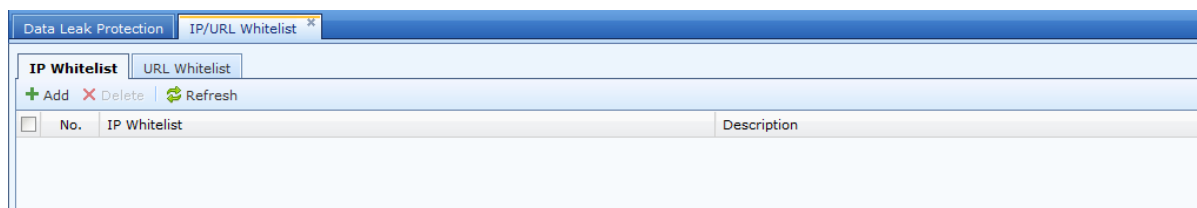


Predefined Sensitive Keyword

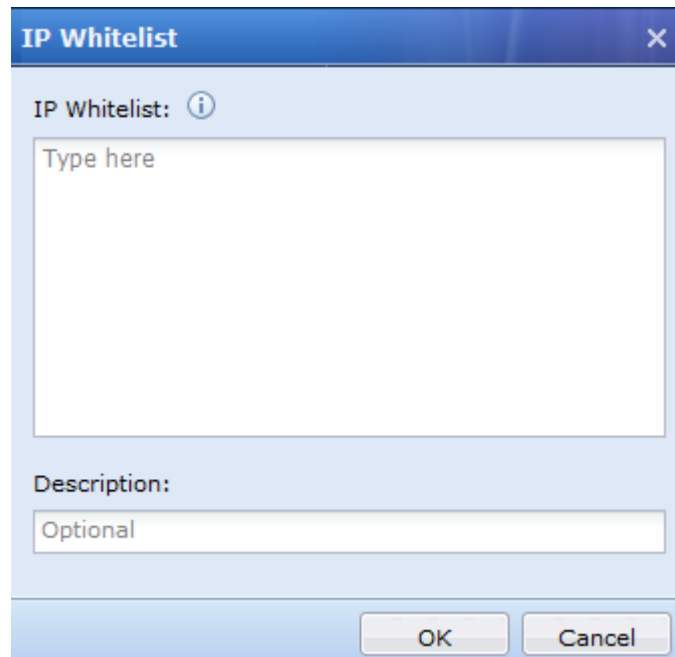
The **Predefined Sensitive Keyword** tab page displays the regular expressions of some sensitive keywords embedded in the equipment, such as the ID number, MD5, and mobile phone number. The embedded sensitive keywords cannot be edited or deleted. Online upgrade is supported. See the figure below.



Click [IP/URL Whitelist](#) to exclude certain IP addresses and URLs from data leak protection. See the figure below.



Click **Add**. The **IP Whitelist** dialog box is displayed, as shown below.



IP Whitelist [X]

IP Whitelist: ⓘ

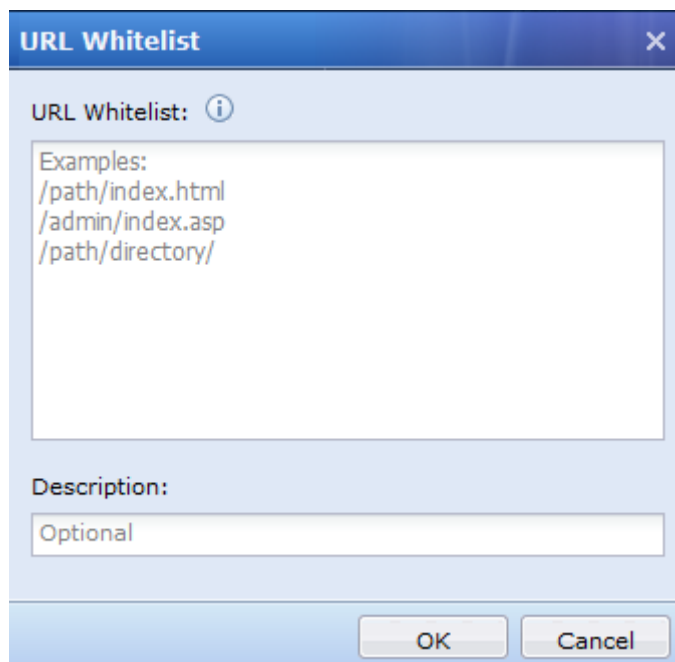
Type here

Description:

Optional

OK Cancel

Select **URL Whitelist** and then click **Add**. The **URL Whitelist** dialog box is displayed, as shown below.



URL Whitelist [X]

URL Whitelist: ⓘ

Examples:
/path/index.html
/admin/index.asp
/path/directory/

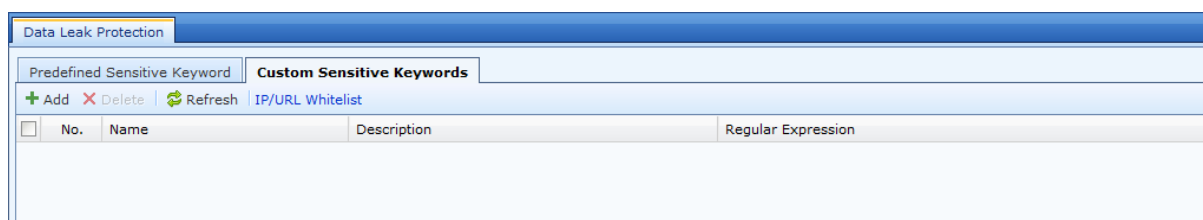
Description:

Optional

OK Cancel

Custom Sensitive Keywords

You can define sensitive keywords on the **Custom Sensitive Keywords** tab page. See the figure below.



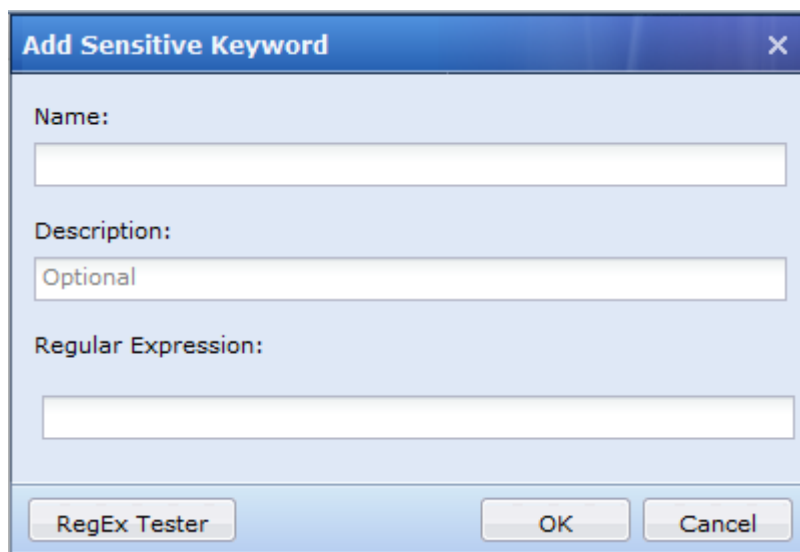
Data Leak Protection

Predefined Sensitive Keyword | **Custom Sensitive Keywords**

+ Add -X Delete ↻ Refresh | IP/URL Whitelist

<input type="checkbox"/>	No.	Name	Description	Regular Expression

Click **Add**. In the displayed **Add Sensitive Keyword** dialog box, enter the regular expression of the sensitive keyword to be defined. See the figure below.



The dialog box titled "Add Sensitive Keyword" has a close button (X) in the top right corner. It contains three text input fields: "Name:", "Description:" (with the placeholder text "Optional"), and "Regular Expression:". At the bottom, there are three buttons: "RegEx Tester", "OK", and "Cancel".

Click **IP/URL Whitelist** to exclude certain IP addresses and URLs from data leak protection. The functions of **IP/URL Whitelist** are the same as that on the **Predefined Sensitive Keyword** tab page.

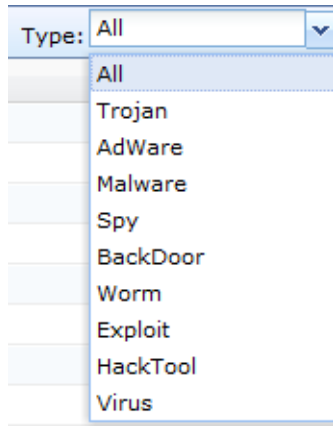
Malware Signature Database

The malware signature database contains a variety of protection types including Trojan, AdWare, Malware, Spy, Backdoor, Worm, Exploit, HackTool and Virus. See the figure below.

Malware Signature Database				
<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable		Action: All	Type: All	Rule ID
<input type="checkbox"/> Rule ID	Signature Name	Type	Threat Level	Action
<input type="checkbox"/> 30000000	Trojan.Win32.Pirminay	Trojan	Medium	Enable
<input type="checkbox"/> 30000001	TR/Downloader.Gen	Trojan	Medium	Enable
<input type="checkbox"/> 30000002	Troj/LdMon-A	Trojan	Low	Enable
<input type="checkbox"/> 30000003	Trojan-Downloader.Win32.Dapato	Trojan	Low	Enable
<input type="checkbox"/> 30000004	Trojan-Downloader.Win32.Dapato	Trojan	Low	Enable
<input type="checkbox"/> 30000005	Trojan-Downloader.JS.Iframe	Trojan	High	Enable
<input type="checkbox"/> 30000006	TR/Graftor.Elzob.15338	Trojan	Low	Enable
<input type="checkbox"/> 30000007	Trojan.Win32.Jorik.Pirminay	Trojan	Medium	Enable
<input type="checkbox"/> 30000008	TR/Graftor.Elzob.15338	Trojan	Low	Enable
<input type="checkbox"/> 30000009	Troj/LdMon-A	Trojan	Low	Enable
<input type="checkbox"/> 30000010	TR/Downloader.Gen	Trojan	High	Enable
<input type="checkbox"/> 30000011	TR/Graftor.Elzob.15338	Trojan	Low	Enable
<input type="checkbox"/> 30000012	Trojan-Banker.Win32.Banker	Trojan	High	Enable
<input type="checkbox"/> 30000013	Trojan.Win32.Yakes	Trojan	Medium	Enable
<input type="checkbox"/> 30000014	Trojan.Win32.Yakes	Trojan	Medium	Enable
<input type="checkbox"/> 30000015	TR/Graftor.Elzob.15338	Trojan	Low	Enable
<input type="checkbox"/> 30000016	Trojan-Dropper.Win32.Daws	Trojan	Low	Enable

You can view all enabled or disabled rules.

The malware signature database contains a variety of protection types including Trojan, AdWare, Malware, Spy, Backdoor, Worm, Exploit, HackTool and Virus.



You can click **Enable** to enable a selected rule.

You can click **Disable** to disable a selected rule.

Custom Rules

Custom Rules contains **Custom WAF Signature** and **Custom IPS Rule**. See the figure below.



Custom WAF Signature

Click **Add** to add new Custom WAF Signature in “Custom WAF Signature”.

Add Web Application Protection Rule

Rule ID: 13990000

Rule Name:

Description: Type here

Impacts: Type here

Threat Level: High

Action: Enable. Block if attack detected

Character String: Match all data ☐ Case Sensitive

Regular Expression: Match all data ☐ Case Sensitive RegEx Tester

Direction: Request

Save and Add OK Cancel

Rule Name, **Description** and **Impacts** can be defined by user.

Threat Level: Able to select High, Medium and Low.

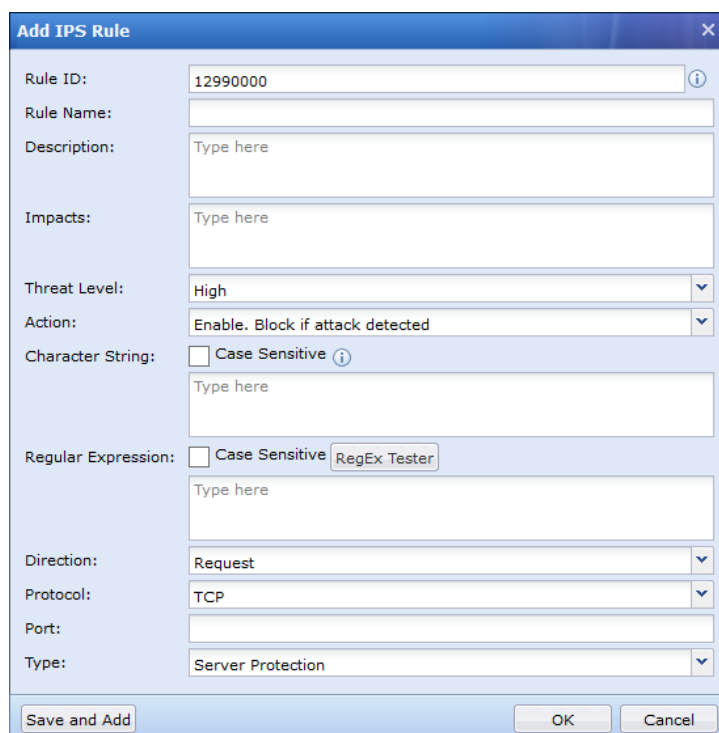
Action: The 3 actions are **[Enable. Block if attack detected]**, **[Enable. Allow if attack detected]** and **[Disable]**.

Character String, **Regular Expression** and **Direction** are used to configure Rule content, first 2 fields can be left blank.

Enable. Allow if attack detected: Attack will be logged and allowed.

Custom IPS Rule

Click **Add** to add new IPS rule in “Custom IPS Rule”.



Rule Name, **Description** and **Impacts** can be defined by user.

Threat Level: Able to select High, Medium and Low.

Action: The 3 actions are [**Enable. Block if attack detected**], [**Enable. Allow if attack detected**] and [**Disable**].

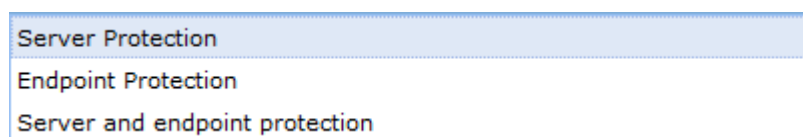
Enable. Block if attack detected: Attack will be logged and blocked.

Enable. Allow if attack detected: Attack will be logged and allowed.

Disable: Disable the selected rule, NGAF will not use this rule.

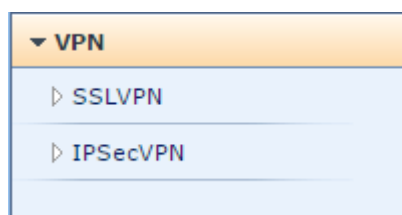
Character String, **Regular Expression** and **Direction** are used to configure Rule content, first 2 fields can be left blank.

Type: Select which target should IPS protect. See the figure below.



VPN

The VPN module allows you to configure the VPN function and view the VPN connection status. Basically the VPN module has 2 types of VPN: **SSLVPN** and **IPSecVPN** as shown in the figure below:

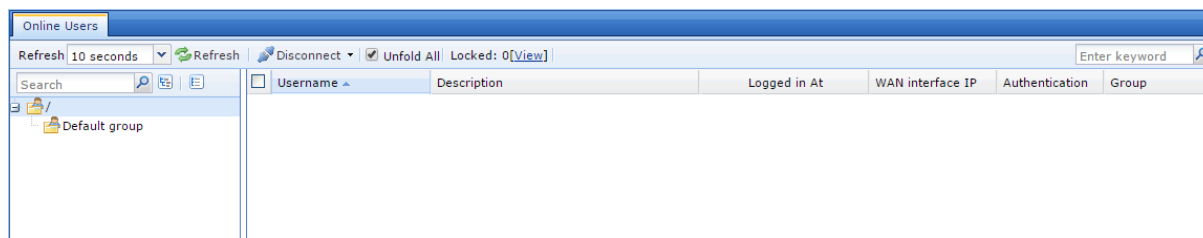


The difference between these 2 types are SSLVPN is mainly for mobile users to connect to NGAF and IPSecVPN is used for connection to branch connection. IPSecVPN consists of SangforVPN and standard IPSecVPN.

SSLVPN

Online Users

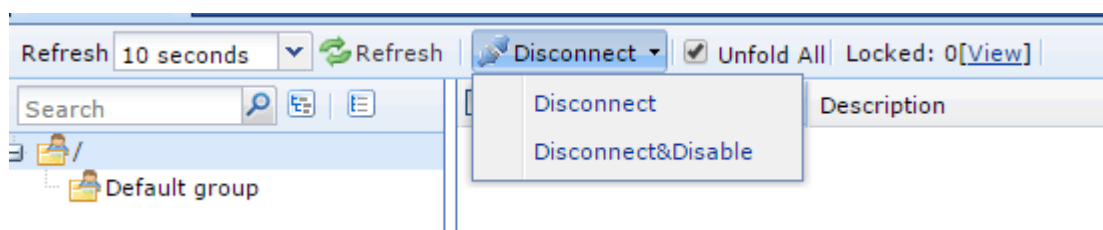
The **Online Users** page can view information of the online users, such as number of users connecting to the SSL VPN, the time when these online users connected, the mount of received/sent bytes, as well as the outbound and inbound speed. Administrator can disconnect or disable any of these online users. The Online Users page is as shown below:



The following are the contents included on Online Users page: □

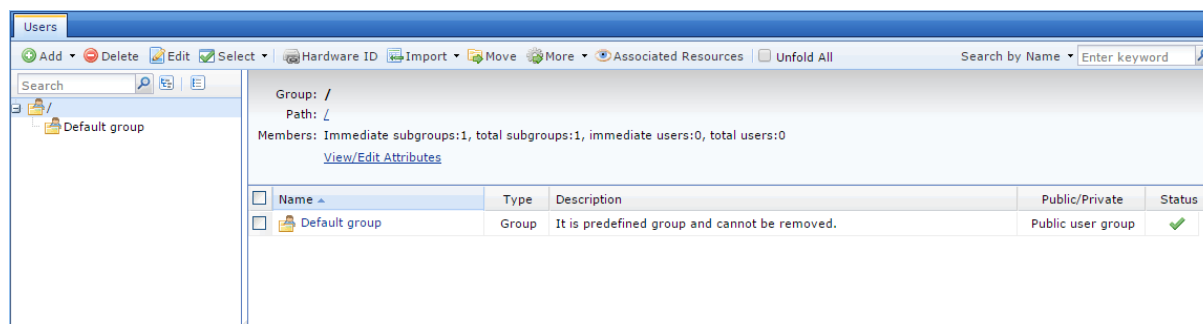
Auto Refresh: Specifies the time interval for refreshing this page, or click **Refresh** to refresh the page manually and immediately. □

Disconnect: Click it and select an option to disconnect, or disconnect and disable the selected user(s), as shown below:



Users

Users and groups are managed in a hierarchic structure. The users with similar attributes could be classified into a group which is further included in another higher-level user group. This kind of management is similar to and compatible with the interior organization structure of an enterprise, facilitating management of VPN users. User Management page is shown below:



In the left pane, there is a tree of user groups. Click on a group name, and the subgroups and direct users of that group will be seen in the right pane, with group information (Group, Location, number of members) displaying above right pane.

To search for a group, enter keyword of the group name into the **Search** fielding the left pane and click the magnifier icon. The group will be highlighted in bold if found.

To see all direct and indirect users of the selected group, click **Unfold All**.

To delete the selected user or group, click **Delete**.

To choose the desired entries, click **Select > Current page** or **All pages**.

To deselect entries, click **Select > Cancel**.

To edit the attributes of a user or group, select the user or group and click **Edit** to enter the **Edit User or Edit User Group** page.

Adding Group

1. Click **Add > Group** to enter Add User Group page, as shown in the figure below:

2. Configure **Basic Attributes** of the user group. The following are basic attributes: □

Name : Enter a name for this user group. This field is required. □

Description : Enter brief description for this user group. □

Added To : Select the user group to which this user group is added.

Max Concurrent Users : Indicates the maximum number of users in this group that can concurrently access SSL VPN. □

Status : Indicates whether this user group is enabled or not. Select **Enabled** to enable this group; otherwise, select **Disabled**.

Inherit role and authentication settings : Select the checkbox next to it and this user group will inherit the attributes such as the roles and authentication settings.

Inherit authentication settings : Select the checkbox next to it and this user group will inherit the authentication settings of its parent group.

Inherit assigned roles : Select the checkbox next to it and the current user group will inherit the assigned roles of its parent group.

3. Configure **Authentication Settings**

Group Type : Specifies the type of this user group, **Public group** or **Private group**. □

Public group : Indicates that any user account in this group can be used by multiple users to log in to the SSL VPN concurrently. □

Private group : Indicates that multiple users to log in to the SSL VPN concurrently can use none of the user accounts in this group. If a second user uses a user account to connect SSL VPN, the previous user will be forced to log out. □

Primary Authentication : Indicates the authentication method(s) that is (are) firstly applied to verify user when he or she logs in to the SSL VPN. If any secondary authentication method is selected, primary authentication will be followed by secondary authentication when the users log in to the SSL VPN. By default is **Local password**.

Local password : The connecting users need to pass local password based authentication, using the SSL VPN

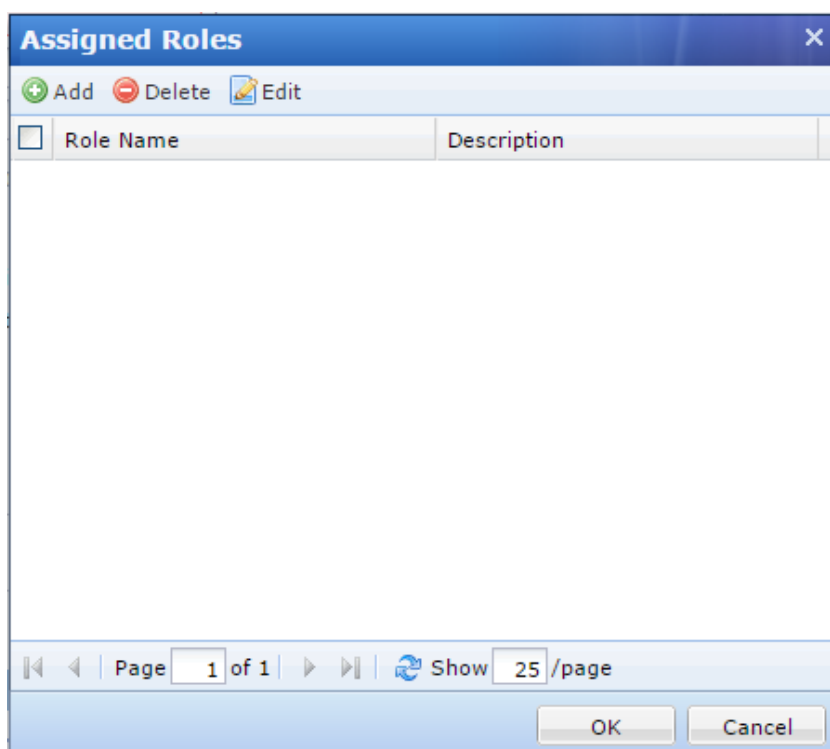
account in this user group.

Secondary Authentication : Secondary authentication is optional and supplementary authentication methods. Select it to require the connecting users to submit the corresponding credentials after he or she has passed the primary authentication(s), adding security to SSL VPN access. □

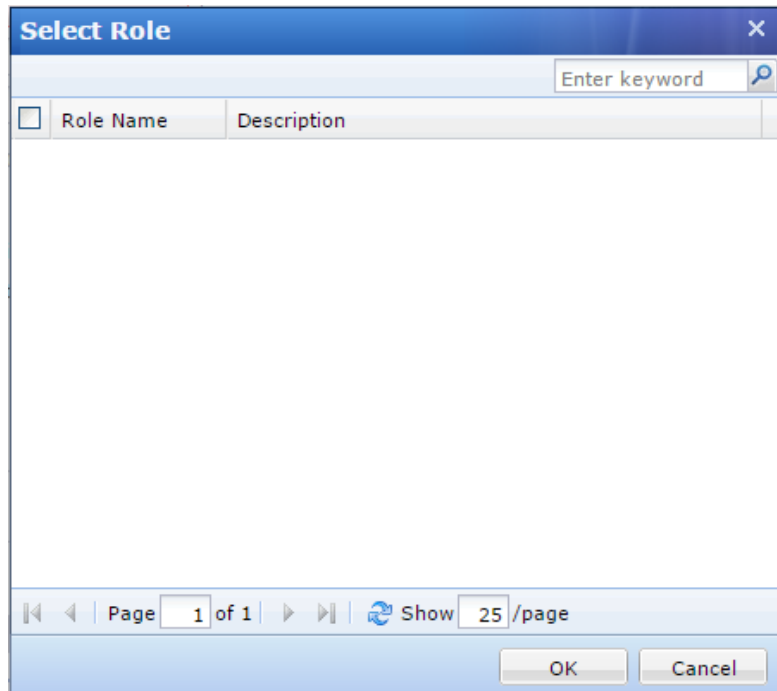
Hardware ID : This is the unique identifier of a client-end computer. Each computer is composed of some hardware components, such as NIC, hard disk, etc., which are unquestionably identified by their own features that cannot be forged. SSL VPN client software can extract the features of some hardware components of the terminal and generate the hardware ID consequently. This hardware ID should be submitted to the Sangfor device and bind to the corresponding user account. Once administrator approves the submitted hardware ID, the user will be able to pass hardware ID based authentication when accessing SSL VPN through specified terminal(s). This authentication method helps to eliminate potential unauthorized access. As mentioned above that multiple users could use a same user account (public user account) to access SSL VPN concurrently, it is reasonable that a user account may bind to more than one hardware IDs. That also means, an end user can use one account to log in to SSL VPN through different endpoints, as long as the user account is binding to the hardware IDs submitted by the user from those endpoints.

4. Assign **roles** to user group.

a. Click on **Roles** field to enter the **Assigned Roles** page, as shown below:



b. Click **Add** to enter the **Select Role** page, as shown below:



- c. Select the checkbox next to the desired roles and click the **OK** button. The roles are added in to the **Assigned Roles** page.
- d. Click the **OK** button and name of the assigned roles filled in the **Roles** field.
- e. If the desired role is not found in the list, click **Create + Associate** to create a new role and associate with the user group. (The procedures of creating a role is the same as that in Roles Adding section).
- f. To remove a role from the list, select the role and click **Delete**.
- g. To edit a role, select the role and click **Edit**.

Adding User

1. Click **Add** and select **User** to enter the **Add User** page, as shown in the figure below:

2. Configure **Basis Attributes** of user. The following are the basic attributes: ☐

Name : Enter a name for this user. This field is required. ☐

Description : Enter brief description for this user. ☐

Added To : Select the user group to which this user is added.

Local Password, Retype Password : Enter the password of this user account. ☐

Mobile Number : Enter the mobile phone number of the user.

Added To : Specifies to which user group this user is added. ☐

Inherit authentication settings parent group : If selected, the current user will inherit its parent group's policy set and authentication settings. If not selected, the authentication settings and policy set could be different from those of its parent group.

3. Configure valid time of the user account. **Expire** indicates the date on which this user account will get invalid. If Never is selected, the user account will be valid always. If On date is selected, select a date as expiry date.

4. Configure **status** of the user account. This user account will be enabled (valid) if Enabled is selected or disabled (invalid) if Disabled is selected.

5. Configure **Authentication Settings**

Public user : Indicate sthat multiple users can use the user account to access SSL VPN concurrently

Private user : Indicates that only one user can use the user account to log in to the SSL VPN at a time. If a second user uses this user account to connect SSL VPN, the previous user will be forced to log out.

Primary Authentication : Indicates the authentication method(s) that is (are) firstly applied to verify user when he or she logs in to the SSL VPN. If any secondary authentication method is selected, primary authentication will be followed by secondary authentication when the users log in to the SSL VPN. By default is **Local password**.

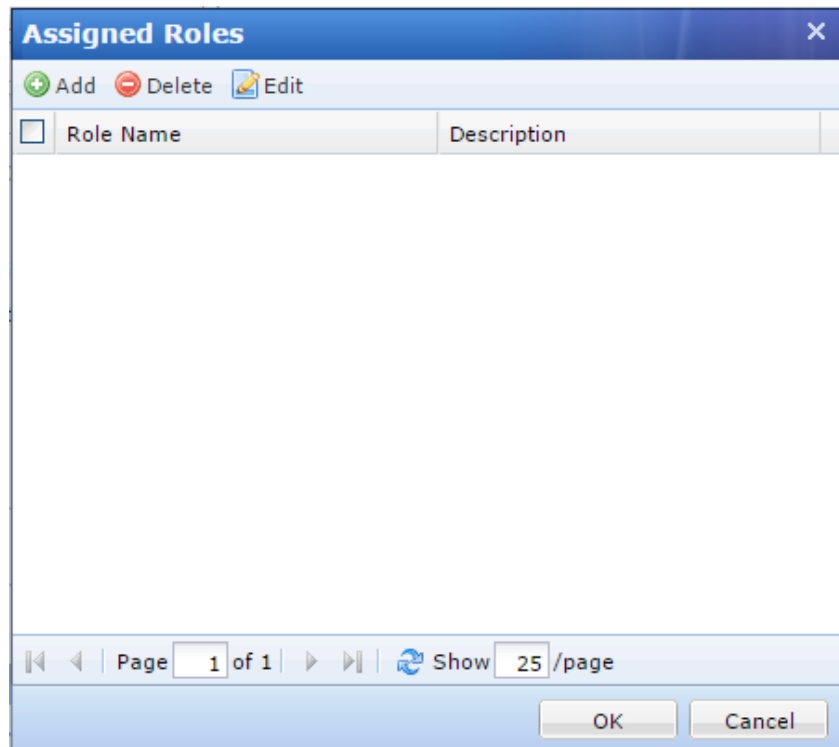
Local password : The connecting users need to pass local password based authentication, using the SSL VPN account in this user group.

Secondary Authentication : Secondary authentication is optional and supplementary authentication methods. Select it to require the connecting users to submit the corresponding credentials after he or she has passed the primary authentication(s), adding security to SSL VPN access. ☐

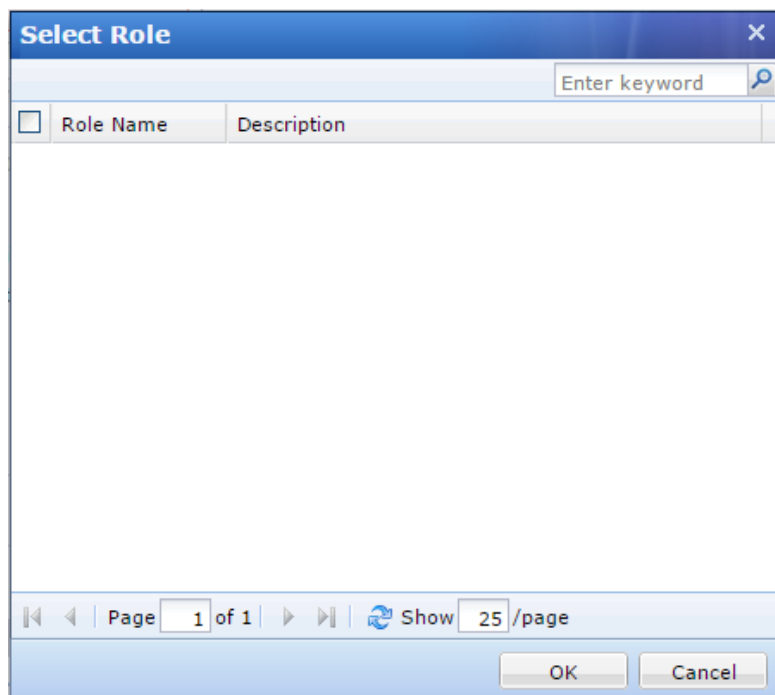
Hardware ID : This is the unique identifier of a client-end computer. Each computer is composed of some hardware components, such as NIC, hard disk, etc., which are unquestionably identified by their own features that cannot be forged. SSL VPN client software can extract the features of some hardware components of the terminal and generate the hardware ID consequently. This hardware ID should be submitted to the Sangfor device and bind to the corresponding user account. Once administrator approves the submitted hardware ID, the user will be able to pass hardware ID based authentication when accessing SSL VPN through specified terminal(s). This authentication method helps to eliminate potential unauthorized access. As mentioned above that multiple users could use a same user account (public user account) to access SSL VPN concurrently, it is reasonable that a user account may bind to more than one hardware IDs. That also means, an end user can use one account to log in to SSL VPN through different endpoints, as long as the user account is binding to the hardware IDs submitted by the user from those endpoints.

6. Assign **roles** to user group.

a. Click on **Roles** field to enter the **Assigned Roles** page, as shown below:



b. Click **Add** to enter the **Select Role** page, as shown below:



c. Select the checkbox next to the desired roles and click the **OK** button. The roles are added in to the **Assigned Roles** page.

d. Click the **OK** button and name of the assigned roles filled in the **Roles** field.

e. If the desired role is not found in the list, click **Create + Associate** to create a new role and associate with the user group. (The procedures of creating a role is the same as that in Roles Adding section).


f. To remove a role from the list, select the role and click **Delete**.

g. To edit a role, select the role and click **Edit**.

Searching for Users

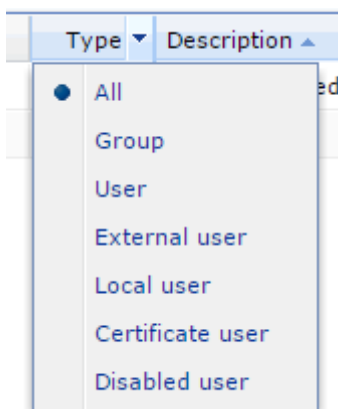
At the upper right of User Management page, there is a **Search** tool intended for searching for user or group, as shown below :




To search for user or group by name, description or mobile number, click and select **Search by xxx**, enter the keyword and click the magnifier icon  or press **Enter** key.

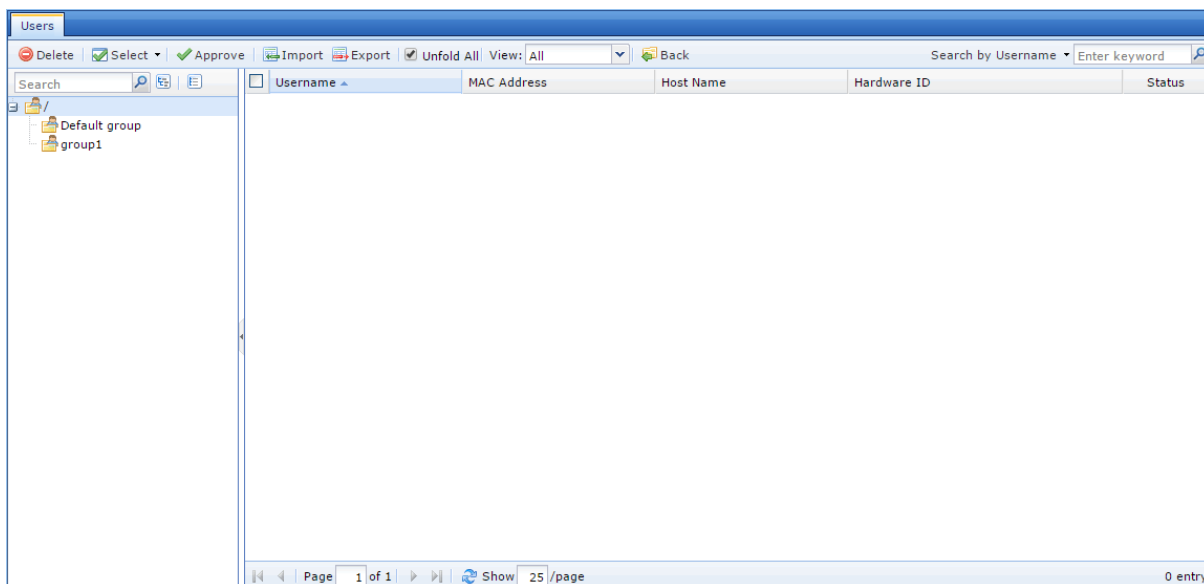
To sort users by name or description, in ascending or descending order, click column header **Name** or **Description**.

To filter users and view only one category of users, click column header **Type**, as shown below:



Managing Hardware IDs

Among the tools on User Management page, there is an item **Hardware ID**  **Hardware ID** . Click it to enter the **Hardware ID** page, as shown below:



The following are some optional operations on Hardware ID page: ☐

Delete : Click it to remove the selected user and/or group. ☐

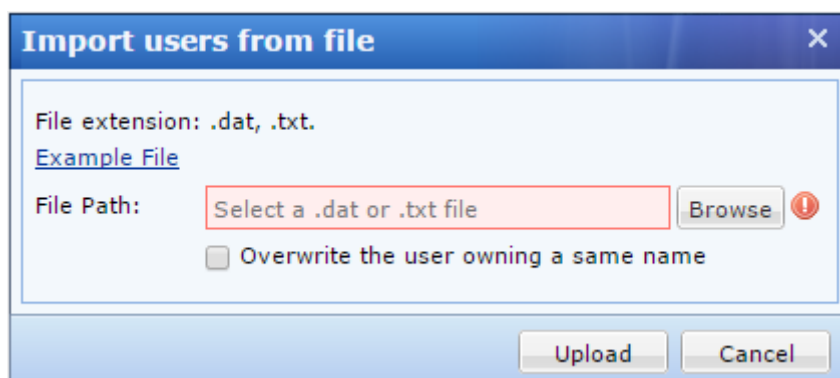
Select : Click **Select** > **On all pages** or **On current page** to select all the hardware IDs or only those showing on the present page; or click **Select** > **Cancel** to deselect users. ☐

Approve : Click it and the selected hardware ID(s) will be approved and the corresponding user will be able to pass hardware ID based authentication. ☐

View : Filter the hardware IDs. Choose certain type of hardware IDs to show on the page, All, The approved or Not approved hardware IDs.

Search : Use the search tool on the upper right of the page, to search for hardware ID based on username or hostname.

Import : Click it to import hardware IDs by hand, as shown below:



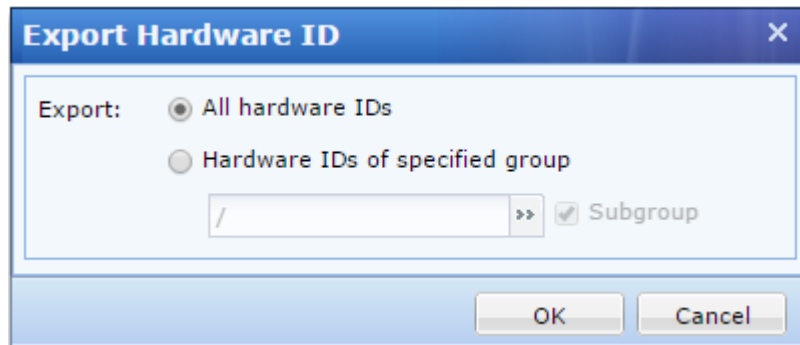
For the file format and the way of maintaining the file that contains hardware IDs, click the **Example File** link to download a copy to the local computer and main the hardware ID as instructed.

Overwrite the user owning a same name : If it happens that any imported user owns the name of an existing user, selection of this option would have that user imported and overwrite the existing user, including hardware ID and other information.

Click the **Browse** button to select a file and then upload button to upload it.

Export : Click it to export the desired hardware IDs and save them into the computer, as shown in the figure

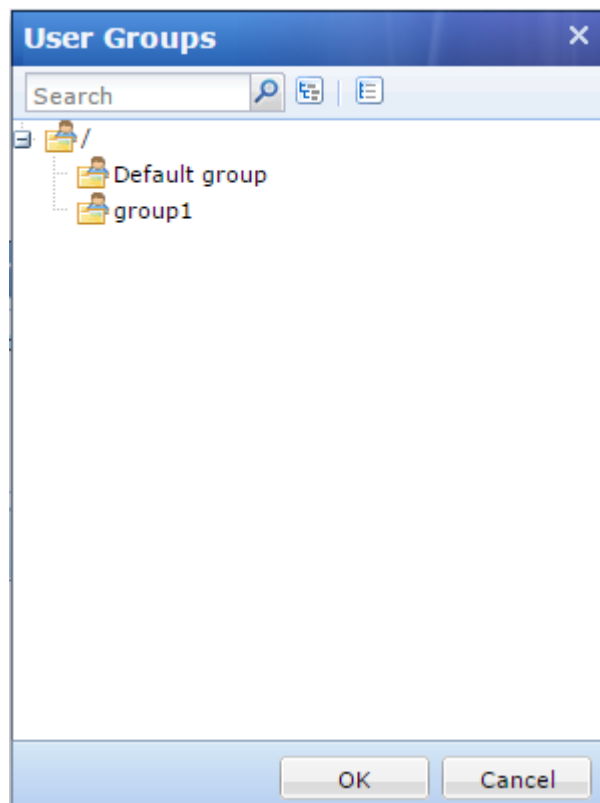
below:



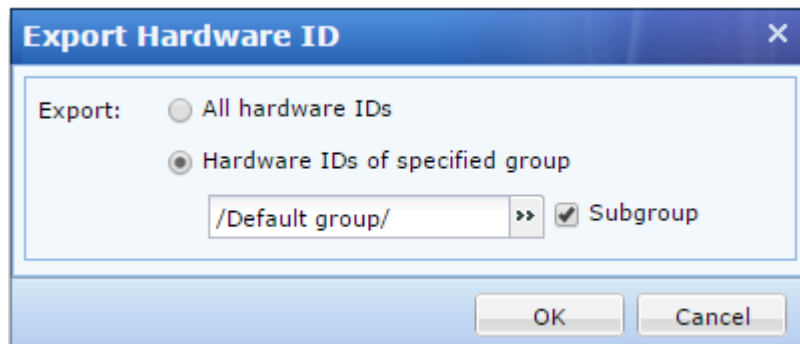
a. Specify the hardware IDs that you want to export.

To export all the hardware IDs, select the option **All hardware IDs** and then click the OK button. All the hardware IDs will be written into a file that will then be saved on the computer.

To export the desired hardware IDs of a specific user group, select **Hardware IDs of specified group** and click the textbox to specify a user group, as shown below:



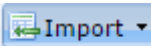
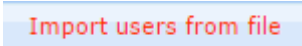
b. Click the **OK** button and the name of the selected user group is filled in the textbox, as shown in the figure below:

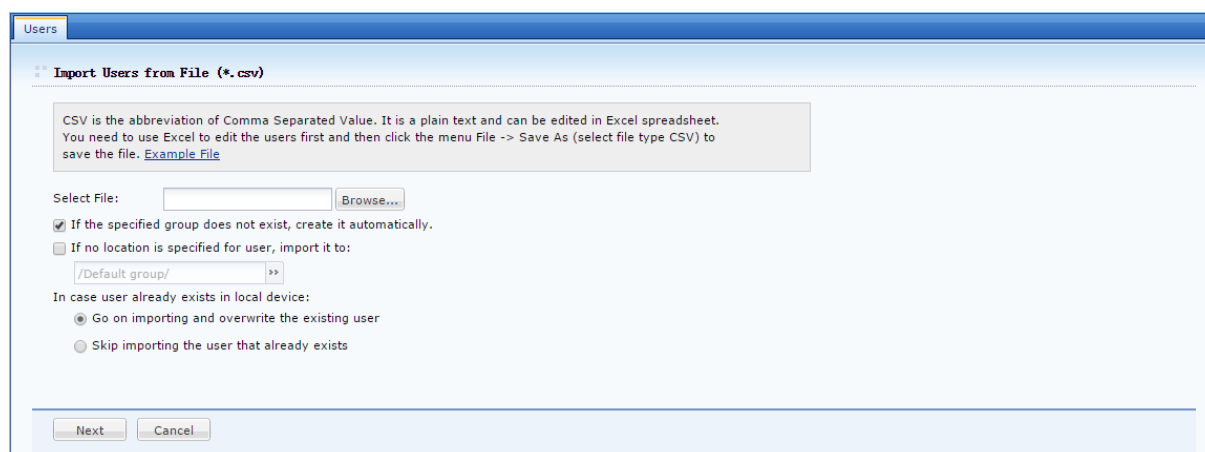


c. To also export the hardware IDs of the users that are included in the subgroups of the specified user group, select the checkbox next to Subgroup included. If this option is not selected, only the hardware IDs of the direct users in the selected group will be exported.

d. Click the **OK** button to write the hardware IDs into a file and download the file into the computer

Importing User to Device

Click on  and select  to import users into NGAF from file as shown in the figure below:



Select File : Browse a CSV file that contains user information, such as username, path, description, password, mobile number, etc., among which the username is required, and others are optional. For more details on how to maintain and edit the CSV file, click the Download Example File link to download a copy and refer to the instructions in it.

If the specified group does not exist, create it automatically : This happens if the Added to Group of some users in the CSV file does not match any of the user groups existing on this Sangfor device.

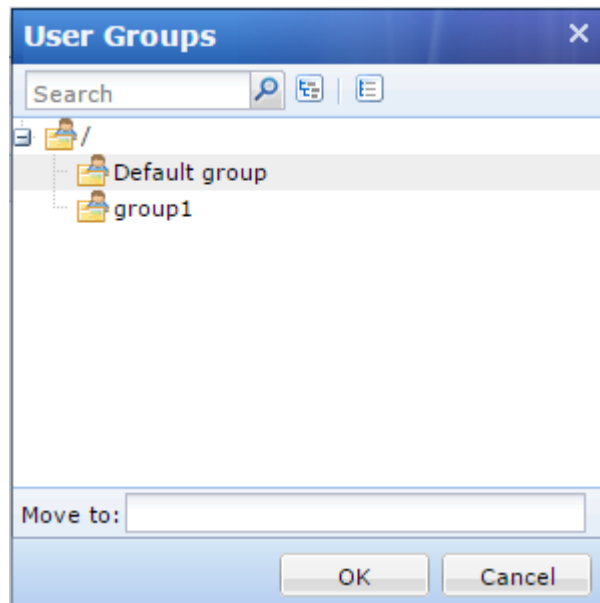
If no location is specified for user, import it to : This specifies the user group to which these users will be added if the Added to Group column is not filled in for some users in the CSV file. □

In case user already exists in local device : This means the imported user's name conflicts with an existing user's name. Select **Go on importing and overwrite the existing user** to overwrite the existing one, or select **Skip importing the user that already exists** not to overwrite the existing one. □

Next : Click it to import the users and add them into the specified user group.

Moving Users to Another Group

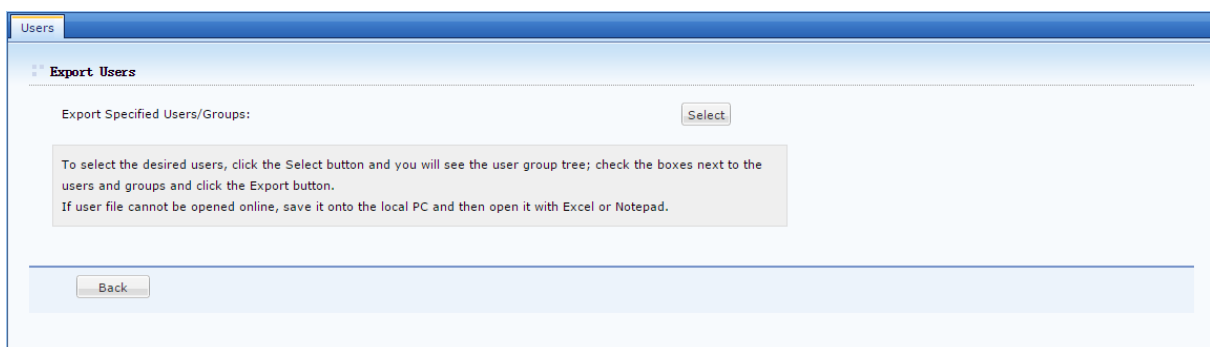
1. On the User Management page, select the desired user/group(s) and click **Move** (on the toolbar) to enter **User Groups** page, as shown below:



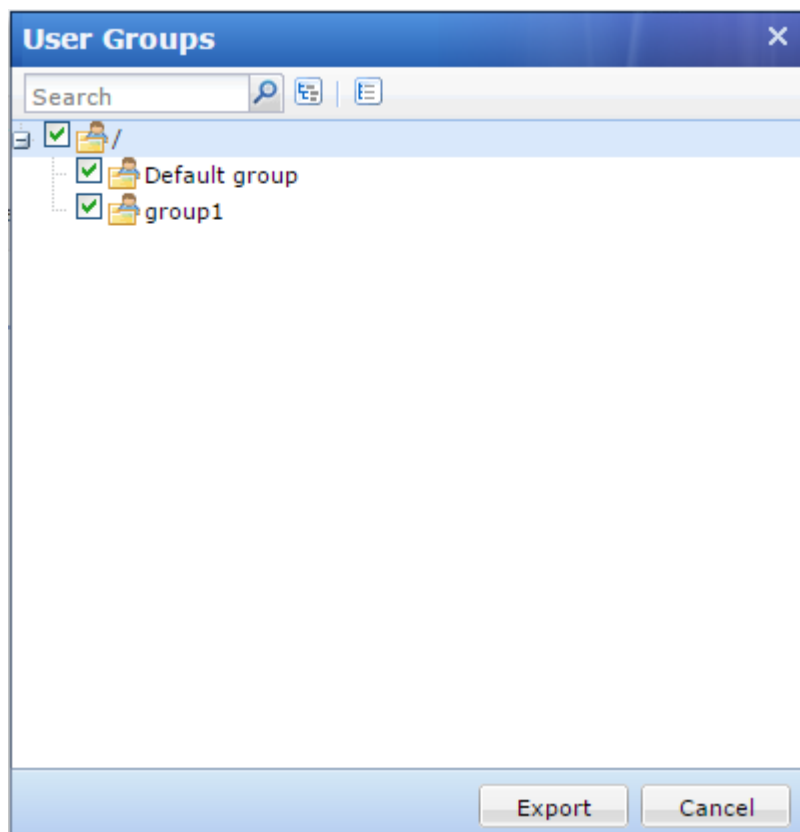
2. Select a user group to which the user/group(s) is added.
3. Click the **OK** button

Exporting Users

1. Click **More > Export** to enter the **Export User File** page, as shown in the figure below:



2. Select the objects that you want to export as shown below :

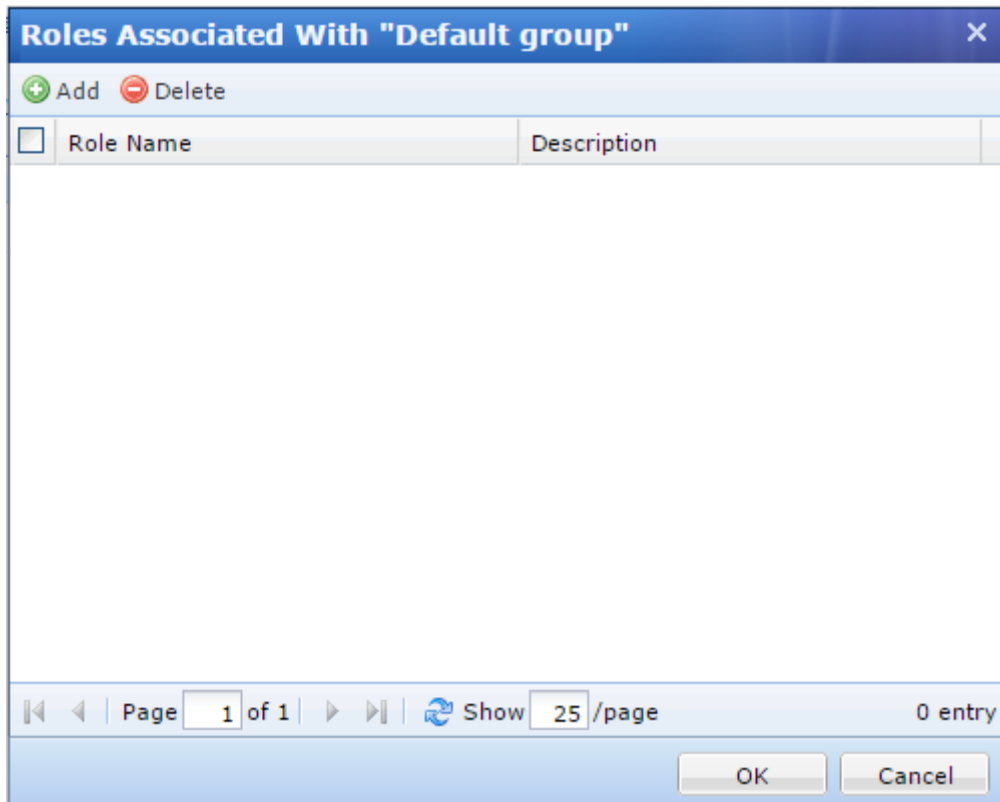


3. Select the desired user group and then click the **Export** button. The selected user will be written into a CSV file and saved on the local computer. The exported user information includes username, group path, password (encrypted by an algorithm developed by SANGFOR), mobile number, description and the time user logged in last time, as shown below:

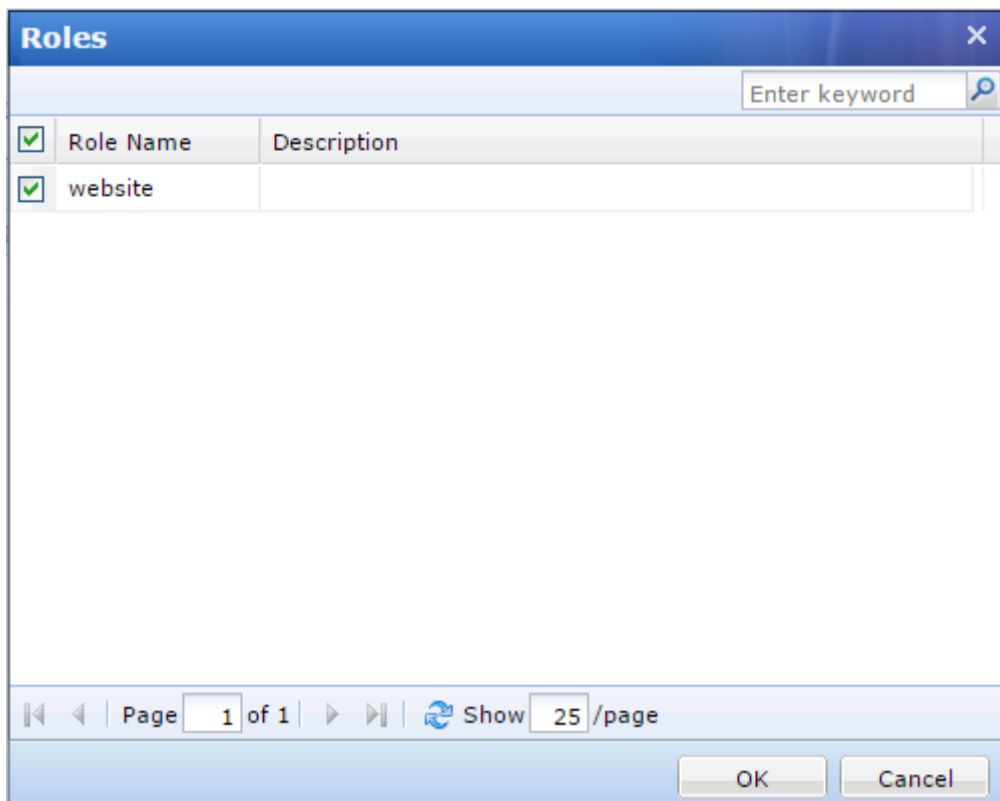
#Username	Added to Group	Password	Mobile Number	Description	Last Login
Leong	/group1	{ 197fba71256ab35f3}	0123456789	normal user	Never logged in
sangfor	/Default group	{ e2cd948b878c5e1d}		test acc	Never logged in

Associating Roles with User

1. Click **More > Associate with role** to enter the **Roles Associated With xxx** page, as shown below:



2. Click **Add** to enter the **Roles** page, as shown in the figure below.



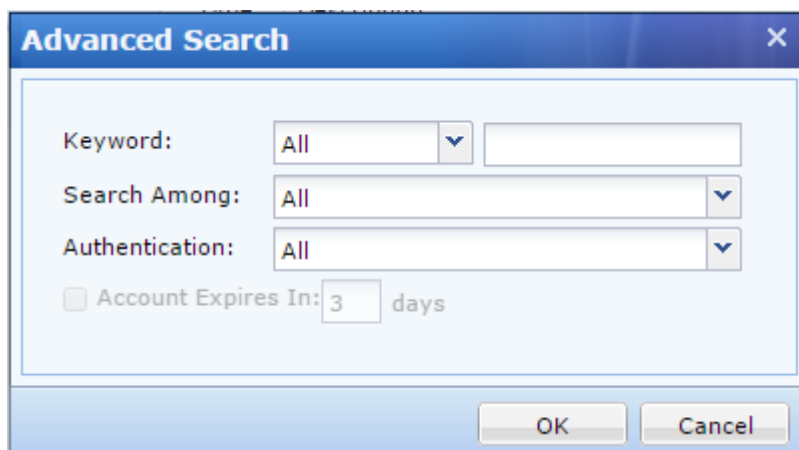
The roles on Roles page are all the roles predefined under SSL VPN>Roles>Role Management.

3. Select the checkboxes next to the roles that you want to associate with the selected user or group.

4. Click the **OK** button and then the Submit button to save the settings.

Advanced Search

Click on **More > Advanced Search** to open advanced search page. The criteria for advanced search are as shown in the figure below:

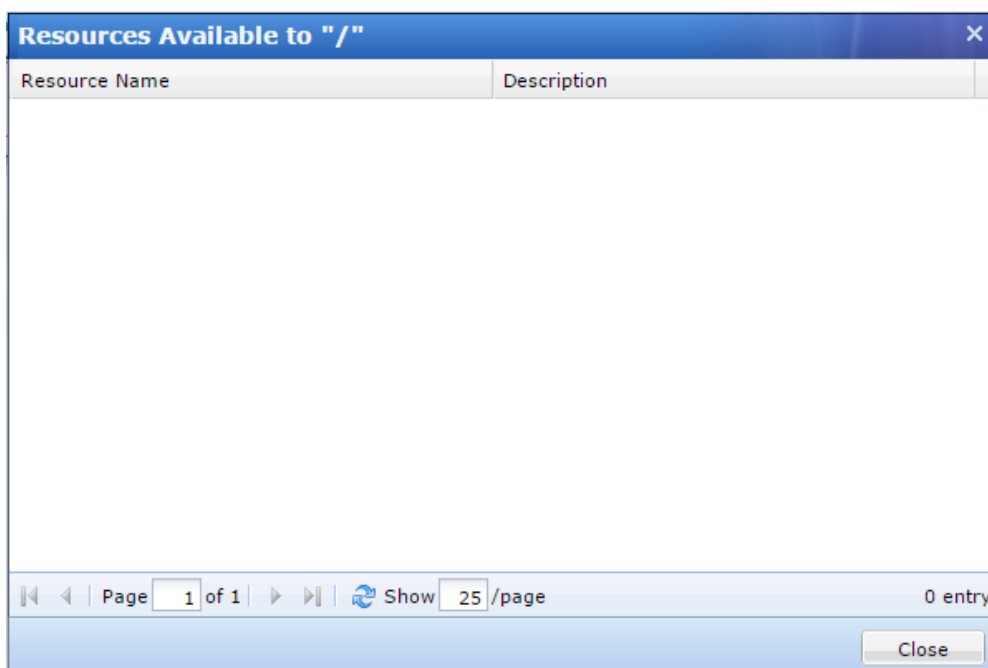


The image shows a dialog box titled "Advanced Search" with a close button (X) in the top right corner. Inside the dialog, there are four search criteria: "Keyword:" with a dropdown menu set to "All" and an adjacent text input field; "Search Among:" with a dropdown menu set to "All"; "Authentication:" with a dropdown menu set to "All"; and a checkbox labeled "Account Expires In:" followed by a text input field containing "3" and the word "days". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Search criteria are keyword, type of keyword, type of users, authentication method and expiry date of the user account.

Viewing Associated Resources of Use

To see what resources are available to certain user or group, select that user or group and click Associated Resource. The resources available to the selected user or group are as shown below:

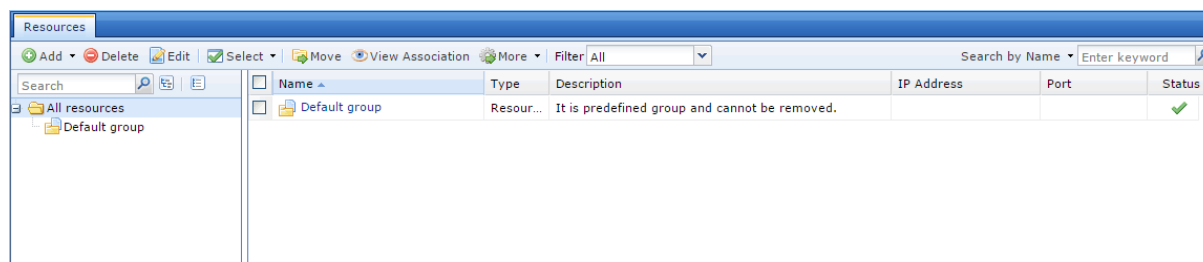


The image shows a dialog box titled "Resources Available to "/" with a close button (X) in the top right corner. The dialog contains a table with two columns: "Resource Name" and "Description". The table is currently empty. At the bottom of the dialog, there is a pagination bar showing "Page 1 of 1", a "Show 25 /page" option, and "0 entry". A "Close" button is located at the bottom right.

Resources

The resources mentioned in this section are the resources that can be accessed by specified users over SSL VPN. The only resource type available for SSLVPN in NGAF is TCP application. Navigate to **SSL VPN > Resources**

and **Resources** page appears, as shown below:



A resource group could contain a number of resources entries. Similar trouser management, resources could be grouped according to categories and associated user or group, etc. Majority of administrators welcomes this kind of management because it makes resources more distinguishable. Navigate to **SSLVPN > Resources > Resource** and click on the resource group, and there sources included in the group are displayed on the right pane. The resource group tree is as shown in the figure on the right. **Default group** is a group protected by system and cannot be deleted, but its attributes could be modified.

Adding/Editing Resource Group

1. Click **Add > Resource Group** to enter Edit Resource Group, as shown in the figure below:

2. Configure Basic Attributes of the resource group. The following are the basic attributes: □

Name, Description : Indicates the name and description of the resource group respectively. This name will be seen on Resource page after user logs in to the SSL VPN successfully.

View resource : Indicates the way resources are displayed on **Resource** page, in icon or in text. If **In Icons** is selected, define the icon size, 48*48, 64*64 or 128*128, so that the resources will be displayed in icon as wanted. If

In Text is selected, you may select **Show description** of the resource.

Added To : Indicates the resource group to which this group is added. By default, resource group added to root group (/).

Adding/Editing TCP Application

TCP application is type of resource that allows end users to use C/S-based or TCP-based application on their local computer to access corporate resources and servers over SSL VPN.

1. Click **Add > TCP app** to enter the **Edit TCP Application** page, as shown in the figure below:

2. Configure Basic Attributes of the TCP application. The following are the basic attributes: □

Name, Description : Indicates the name and description of the TCP resource. This name may be seen on the Resource page after user logs in to the SSL VPN. □

Type : Indicates the type of the TCP application. Some common types are built in the Sangfor device. This selection determines the port number entered in the Port field automatically. If the TCP application is not any of the built-in types, select Other and configure the port manually. □

Address : Indicates the address of the TCP resource. To add one entry of address (IP address, domain name or IP range), click the **Add Address** tab. To add multiple entries of addresses, click the **Add Multiple Addresses** tab, as shown in the figures below :



Port indicates the port used by this TCP application to provide services. For built-in types of TCP applications, this port is predefined. For **Other** type of TCP application, enter the corresponding port number.

Program Path : Indicates path of the client software program that may be used by C/S (client/server) application.

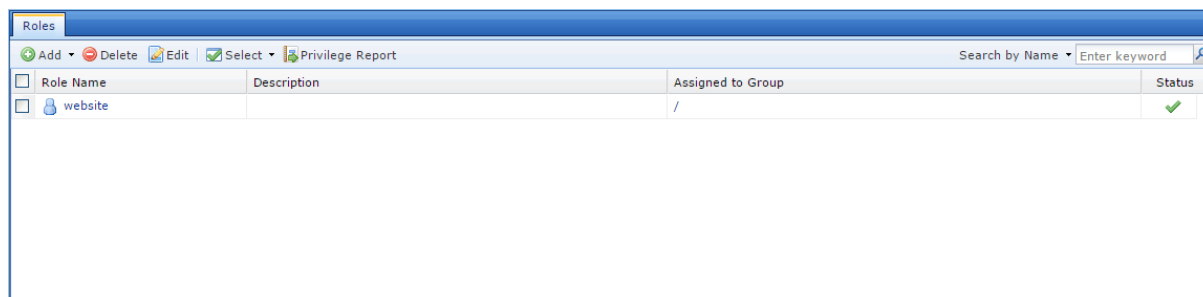
Added To : Indicates the resource group to which this resource is added. By default, the selected resource group is Default group (to configure resource group, refer to the **Adding/Editing Resource Group** section).

Visible for user : To have connecting users see this resource on the Resource page, select this option. Invisibility here only means that the resource is not seen on the Resource page, in fact, it is still accessible to the user.

Roles

A role is an intermediate that builds a connection between **user/group** and **resource**, more specifically, designates

internal resources to user or group. Users can only access the designated internal resources over SSL VPN. This kind of association enables one or multiple users or groups to associate with one or multiple resources, facilitating control over users' access to corporate resources. Navigate to **SSLVPN > Roles** and the **Roles** page appears, as shown below:



The following are some contents included on Role Management page: □

Search by Name/Description/User (Group) : To search for specific role or type of roles, select an option, enter the keyword into the textbox and click the magnifier icon.

Name/description indicates the name/description of the role. **User/group** indicates the user and/or group that the role is assigned to. □

Role Name: Indicates name of the role. □

Description: Indicates description of the role. □

Add: Click it to add new role directly or using an existing role as template. □

Edit: Click it to edit a selected role. □

Delete: Click it to remove the selected role(s).

Adding Role

1. Click **Add > Role** to enter the Add Role page, as shown in the figure below:

Basic Attributes Fields marked * are required

Name: *

Description:

Assigned To:

☒ Enable Role

Associated Resources

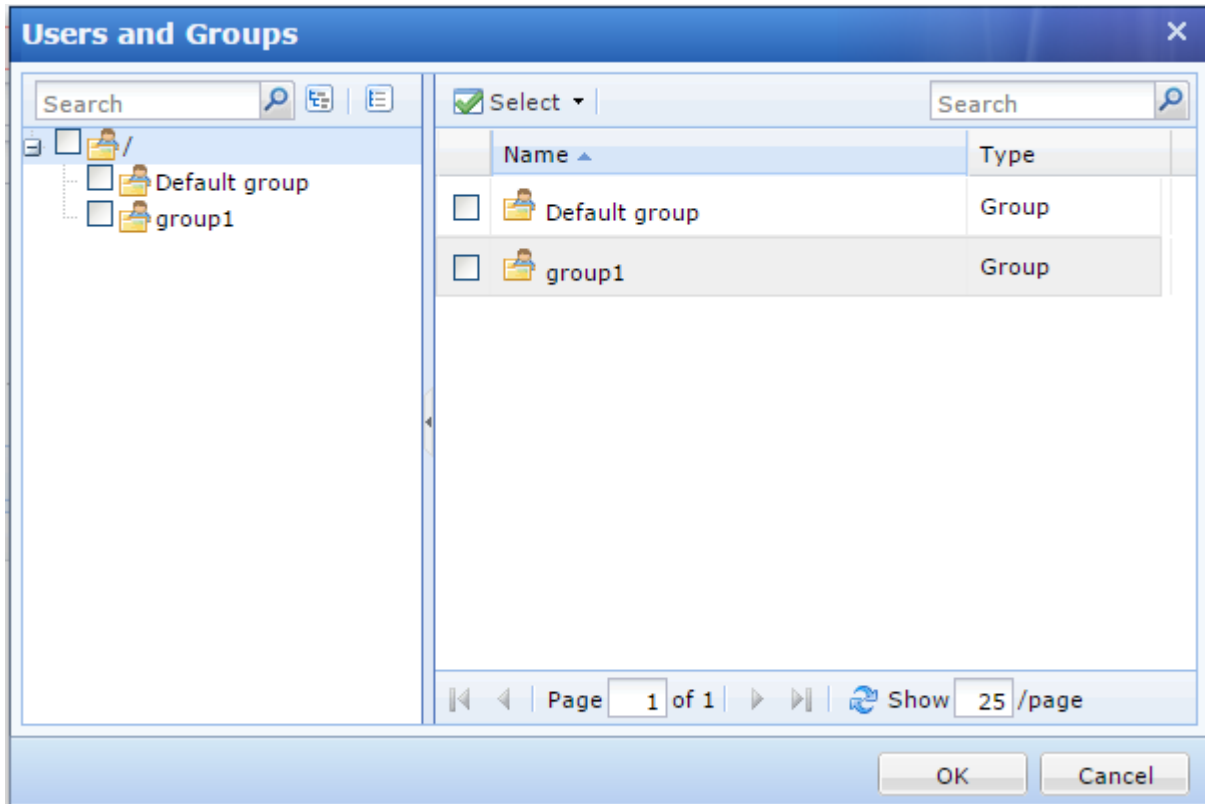
Name	Type	Description
------	------	-------------

2. Configure the Basic Attributes of the role. The following are basic attributes: □

Name : Configures name of the role. ☐

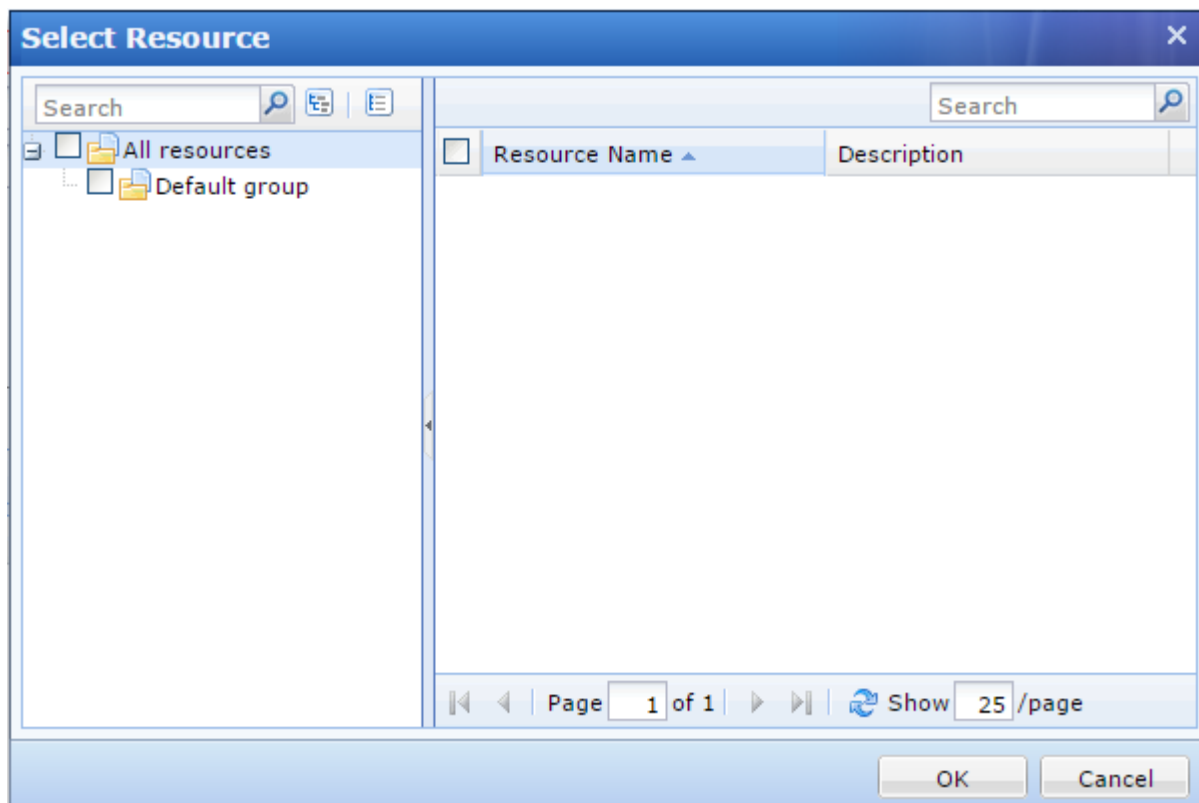
Description : Configures description of the role. ☐

Assigned To : Configures the user and/or group that can access the associated resources. To specify user and group, click the **Select User/Group** button, and all the predefined users and groups on User Management page are seen in the list, as shown below:



Select the user or group to which the role is to be assigned and click the OK button. ☐

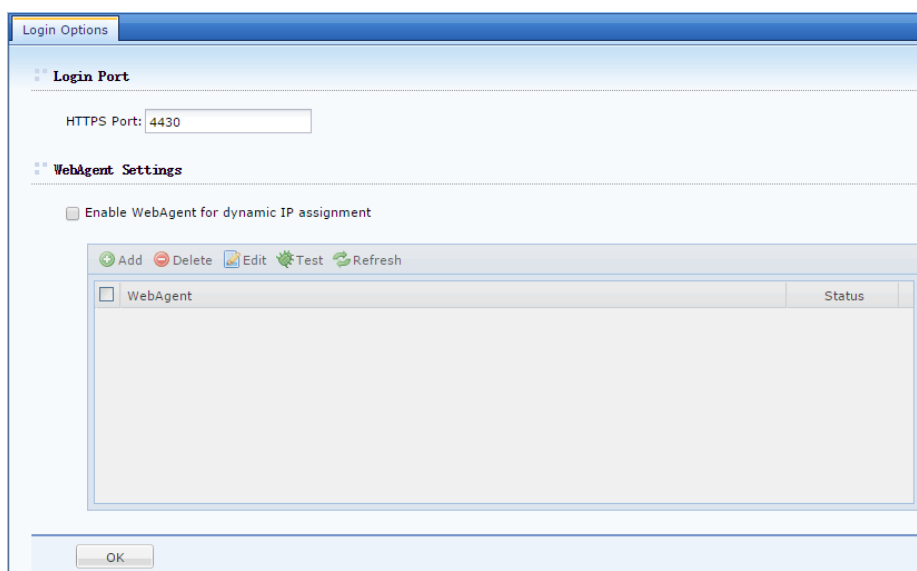
3. Configure associated resources. Click **Select Resources** to enter the Resources page and select resources that the associated users of this role can access, as shown below:



4. Click the **Save** button on the Add Role page to save the settings.

Login Options

Click on **SSLVPN > Login Options** to configure the login port and web agent settings as shown in the figure below:

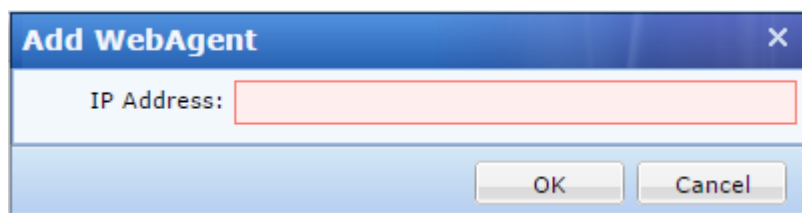


Login Port : Specifies the HTTPS port on which the SSL VPN service is being listened.

Configure Web Agent Settings

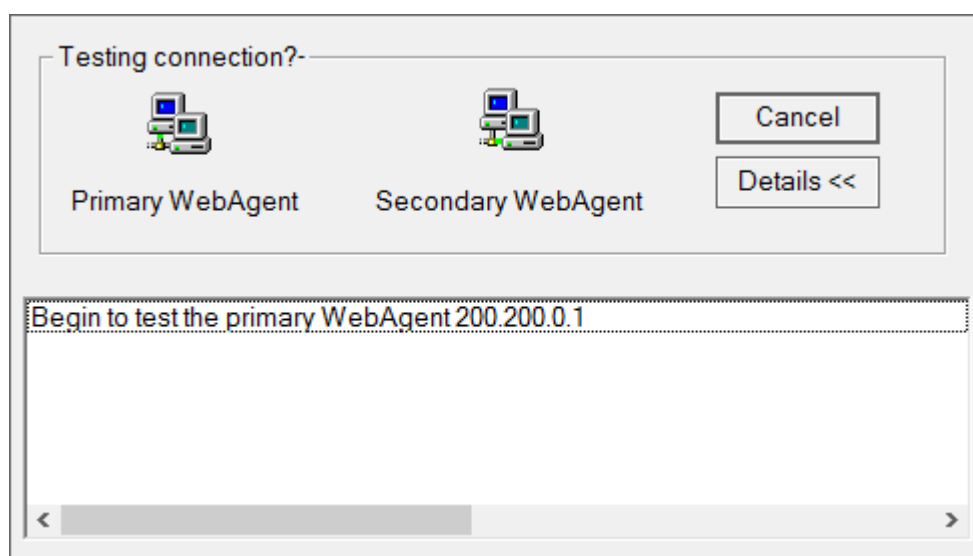
Select Enable Web Agent for dynamic IP support to enable this feature, and the Sangfor device will be able to get an IP using Web Agent dynamic addressing if it is not using a static Internet IP address. To add a Web agent entry:

a. Click **Add** to enter the Add Web Agent page, as shown below:

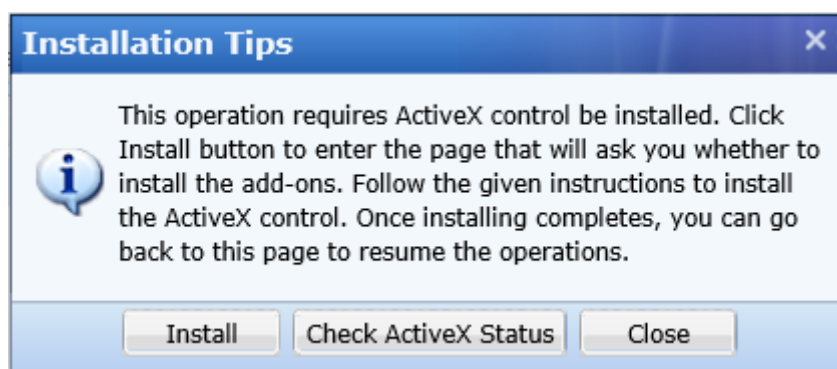


b. Enter the Web Agent address into the Address field and click the **OK** button.

c. To check connectivity of a Web Agent, select a Web Agent and click **Test**. If the address is correct, the Sangfor device then can connect to this Web Agent; otherwise, connecting will fail, as shown in the figure below:



Before test begins, certain ActiveX control may need be installed (as shown below).



d. To remove or edit a Web Agent entry, select the desired entry and click **Delete** or **Edit**.

e. To modify password of a Web Agent select the desire entry and click **Modify PWD**. Modifying password can prevent unauthorized user from using and updating a false IP address into the Web Agent page

f. To refresh the status of the Web Agent, click **Refresh**.

Logging In

Navigate to **SSLVPN > Logging In**. The Logging In Page is as shown in the figure below:

Logging In

Basic Attributes

Fields marked * are required

Page Title:

Access to SSL VPN*

Background Color:

Bulletin Message:

(HTML supported; max 1024 characters)

[\[Preview\]](#)

OK

Cancel

Page Title : Specifies the caption of the login page

Background Color : Indicates the background color of the login page


Bulletin Message : Enter themes age into the textbox. This bulletin message will be seen on the portal after users log in to the SSL VPN. Maximum 1024 characters are allowed and HTML is supported.To preview the bulletin message, click **Preview**.

Authentication

Authentication covers settings related to primary and secondary authentication methods. Navigate to **SSLVPN > Authentication** and the Authentication page appears, as shown in the figure below:

Authentication

Primary Authentication




- Local Password

Settings

Password strength, the ways that users change password, applying only to the user accounts in local database.

Secondary Authentication




- Hardware ID

Settings

Configure hardware ID related options, such as hardware ID collecting and approval.

Other Options



- Password Security Options

Settings

Block insecure and brute-force login.

Primary Authentication Method

The primary authentication method in NGAF is local password based authentication. The settings related to local password based authentication include password security options and username options. Click the **Settings** button following Local Password, and the Local Password Based Authentication page appears, as shown in the figure below:

The screenshot shows a window titled "Authentication" with two main sections. The first section, "Password Security Policy", contains several settings: "Enabled" is checked with a note "(the options only apply to the private users in local database)"; "Password must not contain username" is unchecked; "New password must be different from previous password" is checked; "Minimum length is 6 bytes" is checked; "Every 0 days, user must change password, 0 days before the password expires, remind user to change it" is unchecked; "User must change the initial password (upon the first logon)" is checked; and "Password must have" is checked with sub-options "Digit" (checked), "letter" (checked), and "special character (shift+number key)" (unchecked). The second section, "Username Options", contains "Ignore case of username" which is unchecked. At the bottom are "OK" and "Cancel" buttons.

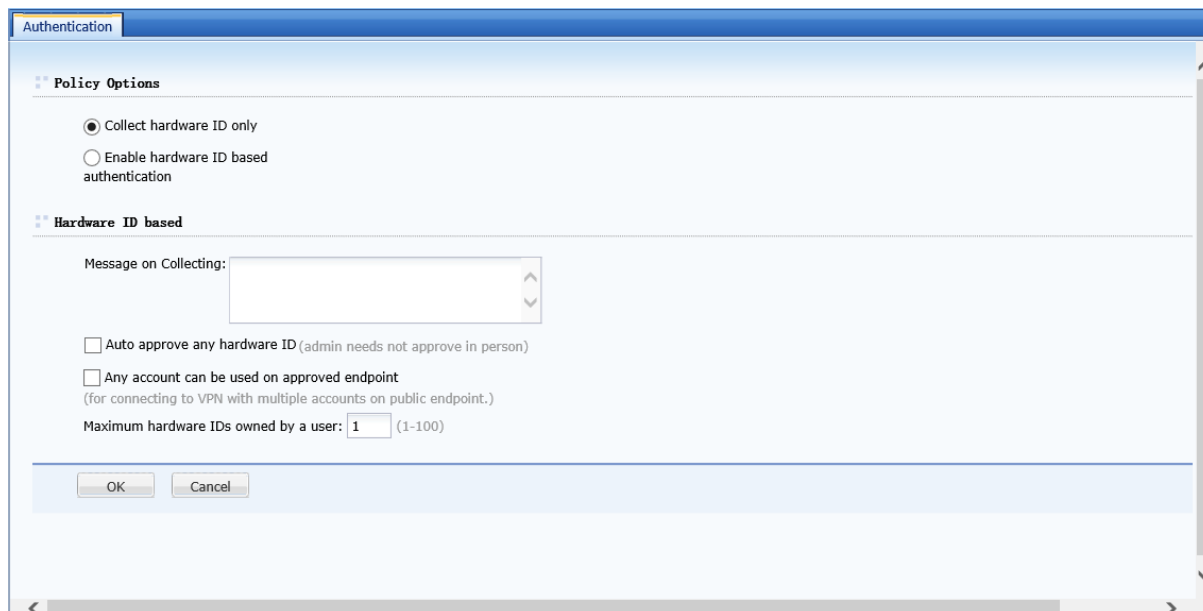
The following are some contents included on the Local Password Based Authentication page: □

Password Security Policy : Configures the password strength, the ways that users change password. □ **Username Options** : If the option **Ignore case of username** is selected, case of username would be ignored when users enter credentials to log in to SSL VPN.

Secondary Authentication Method

The secondary authentication method in NGAF is Hardware ID based authentication.

Hardware ID is a unique serial number generated using the extracted features of hardware components in a computer, according to certain algorithm. The uniqueness of computer components makes the generated hardware ID unique. Click the **Settings** button following Hardware ID and the Hardware ID Based Authentication page appears, as shown in the figure below:



The following are the contents included on Hardware ID Based Authentication page:

Collect hardware ID only : If this option is selected, hardware IDs of endpoint computers will be collected, but hardware ID based authentication will not be enabled.

Enable hardware ID based authentication : If this option is selected, hardware ID of endpoint computers will be collected and hardware ID based authentication enabled.

Message on Collecting : This will turn out to be a prompt seen by end users when they go through hardware ID based authentication.

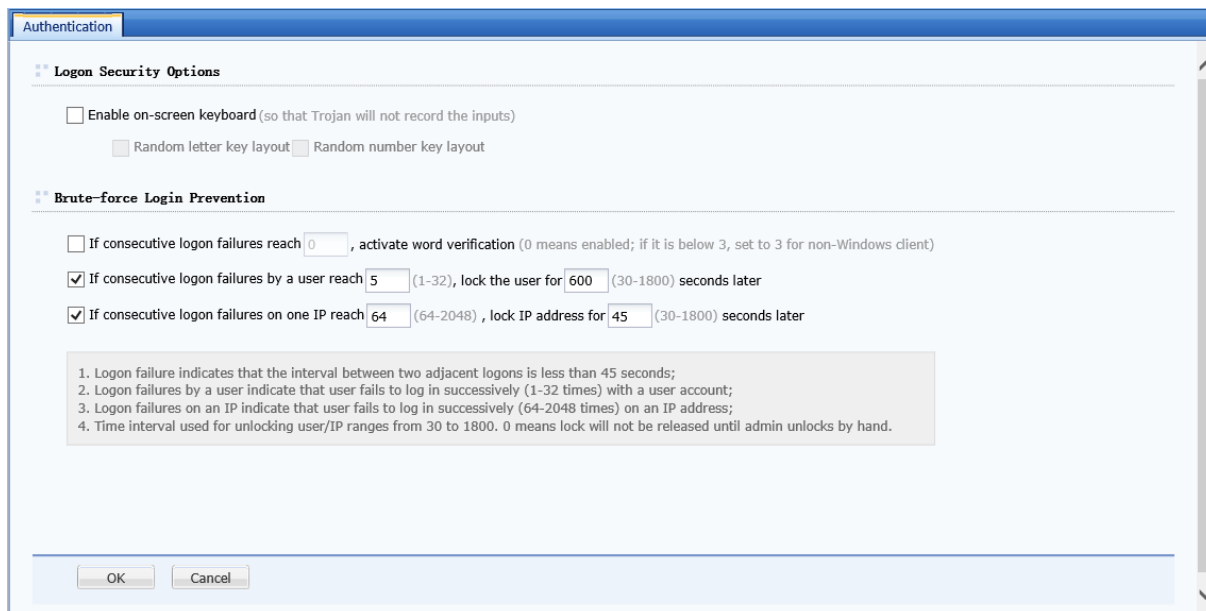
Auto approve any hardware ID : Indicates that any hardware ID submitted by end user will be approved, and administrator need not approve them manually.

Any account can be used on approved endpoint : Indicates that hardware IDs submitted by any user from certain endpoint(s) will be approved automatically if administrator has ever approved the hardware ID of the endpoint(s).

Save : Click this button to save the settings when configuration is completed.

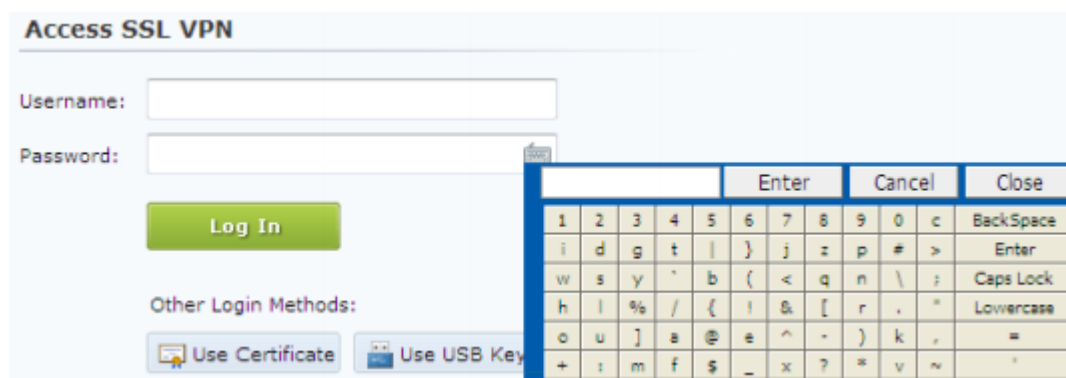
Password Security Options

Password security options are settings related to login when user submits username and password to access the SSL VPN, including two parts, Logon Security Options and Brute-force Login Prevention. Click the **Settings** button following Password Security Options and the Password Security Options page appears, as shown in the figure below:



The following are the contents included on the Password Security Options page :

Enable on-screen keyboard : On-screen keyboard is a virtual keyboard available on the login page to the SSL VPN and can prevent input disclosure, adding security to SSL VPN access. The other two options Random letter key layout and Random number key layout can have the letter keys and number keys on the virtual keyboard change positions randomly every time user uses this keyboard. When user logs in to the SSL VPN and wants to call the on-screen keyboard, he or she needs only to click the keyboard icon next to the Password field on the login page, as shown in the figure below:

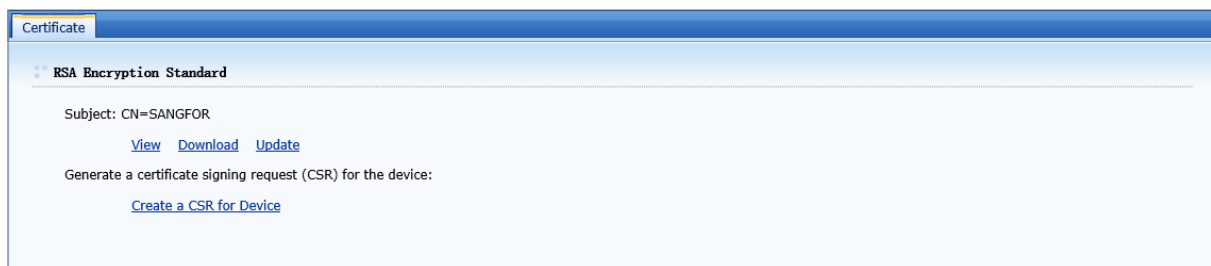


Brute-force Login Prevention : This security feature enables the system to take actions to stop brute-force login attempt. If user fails to log in many times, the login IP address or the user account would be locked up or word verification be enabled for a period of time. The prompt given is as shown below:

The image shows a web interface titled "Access SSL VPN". It contains two input fields: "Username:" and "Password:". Below these fields is a yellow warning box with a red exclamation mark icon. The text inside the box reads: "You are trying brute-force login. The user account is locked!". At the bottom of the interface is a green button labeled "Log In".

Certificate

Certificate is intended for establishing sessions between the Sangfor device and client. To view current certificate of or to generate certificate for the Sangfor device, navigate to **SSLVPN > Certificate**, as shown in the figure below:



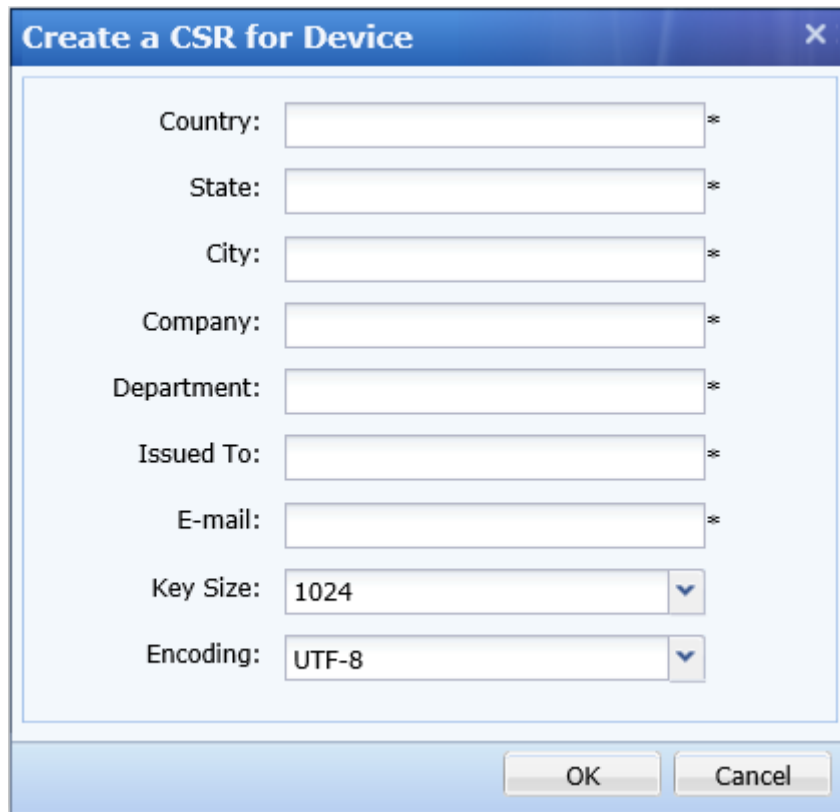
The following are the contents included on the Certificate page:

View : Click it to view the detailed information of the current certificate.

Download : Click it to download the current device certificate.

Update : Click it to import a new certificate to take the place of the current one.

Create CSR for Device : Click this button to generate a certificate-signing request (CSR) which should be sent to the external CA to generate the device certificate. The page is shown in the figure below :



Create a CSR for Device

Country: *

State: *

City: *

Company: *

Department: *

Issued To: *

E-mail: *

Key Size: 1024 ▼

Encoding: UTF-8 ▼

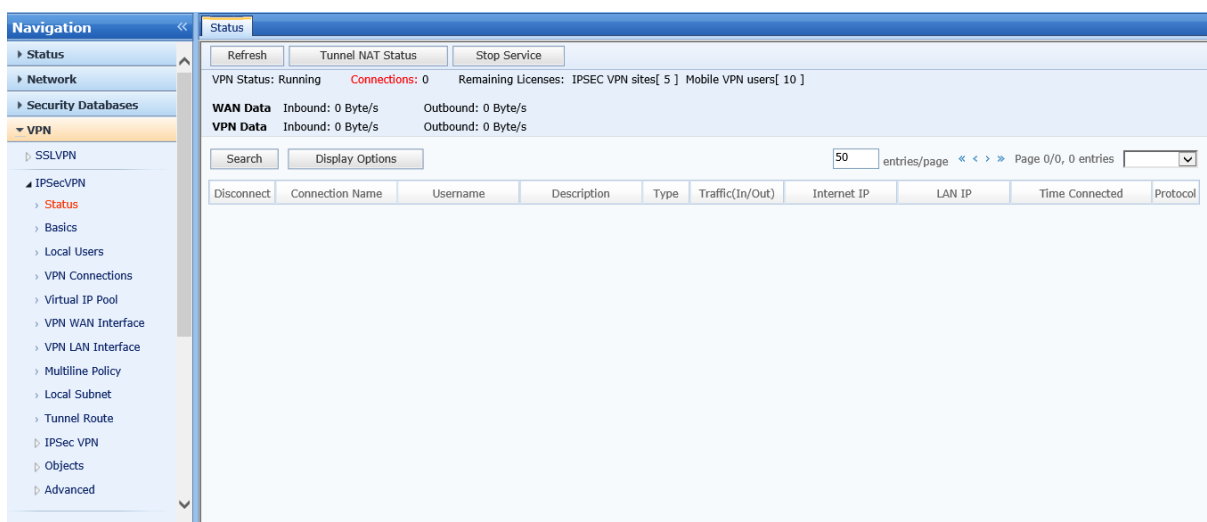
OK Cancel

Configure the required fields and then click the **OK** button.

Once the certificate signing request is generated, click the **Download** Link to download the request. The contents of the downloaded request file are as shown below:

IPSecVPN

The VPN module allows you to configure the Sangfor VPN/IPsecVPN function and view the VPN connection status.



Navigation

- Status
- Network
- Security Databases
- VPN
 - SSLVPN
 - IPSecVPN
 - Status
 - Basics
 - Local Users
 - VPN Connections
 - Virtual IP Pool
 - VPN WAN Interface
 - VPN LAN Interface
 - Multiline Policy
 - Local Subnet
 - Tunnel Route
 - IPSec VPN
 - Objects
 - Advanced

Status

Refresh Tunnel NAT Status Stop Service

VPN Status: Running **Connections:** 0 Remaining Licenses: IPSEC VPN sites[5] Mobile VPN users[10]

WAN Data Inbound: 0 Byte/s Outbound: 0 Byte/s

VPN Data Inbound: 0 Byte/s Outbound: 0 Byte/s

Search Display Options 50 entries/page < > Page 0/0, 0 entries

Disconnect	Connection Name	Username	Description	Type	Traffic(In/Out)	Internet IP	LAN IP	Time Connected	Protocol
------------	-----------------	----------	-------------	------	-----------------	-------------	--------	----------------	----------



To use the VPN function, ensure that at least one layer 3 interface is available on the equipment. The VPN function requires multi-function authorization.

Status

The **Status** page displays current VPN connection and network traffic information. See the figure below.

The screenshot shows the 'Status' page with the following elements:

- Buttons:** Refresh, Tunnel NAT Status, Stop Service.
- VPN Status:** Running, Connections: 0, Remaining Licenses: IPSEC VPN sites[5] Mobile VPN users[10]
- WAN Data:** Inbound: 0 Byte/s, Outbound: 0 Byte/s
- VPN Data:** Inbound: 0 Byte/s, Outbound: 0 Byte/s
- Search:** A search bar with a 'Display Options' button.
- Table:** A table with columns: Disconnect, Connection Name, Username, Description, Type, Traffic(In/Out), Internet IP, LAN IP, Time Connected, Protocol. The table is currently empty.
- Page Info:** 50 entries/page, Page 0/0, 0 entries.

Click **Refresh** to refresh the VPN connection status and traffic status.

Click **Tunnel NAT Status** to view the current tunnel NAT status, including the user name, original subnet segment, proxy subnet segment, network type and subnet mask. See the figure below.

The screenshot shows the 'Tunnel NAT Status' page with the following elements:

- Buttons:** Refresh.
- Summary:** Total Users:0, Total Network Segments NATed:0.
- Search:** A search bar with a 'Display Options' button.
- Table:** A table with columns: No., Username, Source Subnet, Translate to Subnet, Type, Subnet Mask. The table is currently empty.
- Page Info:** Entries Per Page: 50, Page 0/0, 0 entries.

Click **Stop Service** to stop the VPN service temporarily.

Click **Search** and enter a user name to quickly learn the connection condition of the user. See the figure below.

A dialog box with a light blue background. It contains a label "Username:" followed by a text input field. At the bottom, there are two buttons: "Search" and "Cancel".

Click **Display Options** to select the options to be displayed. See the figure below.

A dialog box with a light blue background. It contains a list of options, each with a checked checkbox: "Select All", "Connection Name", "User Name", "Description", "User Type", "Realtime Traffic", "Internet IP", "LAN IP", "Time Connected", and "Protocol". At the bottom, there are two buttons: "Save" and "Cancel".

Basic Settings

The **Basic Settings** page displays Web agent information, MTU value of VPN data, minimum compression value, VPN listening port, VPN connection mode, broadcast packet, and performance settings.

WebAgent specifies the address of the dynamic IP addressing file on the Web server. There are two WebAgent addresses, of which one is primary and the other secondary. See the figure below.

A screenshot of the "Basic Settings" configuration page. The page has a blue header bar with the title "Basic Settings". Below the header, there are several input fields and buttons. On the left, there are fields for "Primary WebAgent" (containing "10.254.254.4009"), "Secondary WebAgent", "MTU (224-2000)" (containing "1500"), "Min Compression Value(99-5000)" (containing "100"), and "VPN Listening Port(default 4009)" (containing "4009"). To the right of these fields are buttons for "Modify Password" (two instances) and "Shared Key". Below the input fields, there are radio buttons for "MSS Change(UDP only)" (with "Allow" selected) and "Internet Connection" (with "Directly" selected). At the bottom of the page, there are three buttons: "Advanced", "Test", and "Save and Apply".

In case of **Dynamic addressing (non-fixed IP address)**, enter the Webpage address of the Web agent, which usually ends with .php. You can click Test to check whether the address is reachable. In case of fixed IP address, enter the Webpage address in the format of IP address:port number, for example, 202.96.134.133:4009. Click **Modify Password** to set the password of the Web agent. This is to prevent unauthorized users from embezzling the Web agent to update a false IP address. Click **Shared Key** to set a shared key. This is to avoid unauthorized access to the equipment.



If a password is set for the Web agent, the password cannot be recovered once lost. In this case, contact SANGFOR customer service center to regenerate a password-free Web agent file and then replace the original file with this new file. If a shared key is set, the same shared key must be set for all VPN sites for interworking purposes. If multiple lines and fixed IP addresses are used, set the address of the Web agent in the format of IP1#IP2:port.

MTU: specifies the maximum MTU value of VPN data. The default value is **1500**.

Min Compression Value: specifies the minimum size of a compressed VPN data package. The default value is **100**.

VPN Listening Port: specifies the listening port of the VPN service. The default value is **4009**. It is configurable.

MSS Change: specifies the maximum VPN data fragment in User Datagram Protocol (UDP) transmission mode.



In normal cases, retain the default values of MTU, Min Compression Value and MSS Change. If you need to change the any value, change it under the guidance of SANGFOR technical support engineers.

Internet Connection: connection mode of the gateway to the Internet. It can be set to **Directly** or **Indirectly**. If Internet users can access the VPN port of the gateway by directly obtaining an Internet IP address or through port mapping, set **Internet Connection** to **Directly**. Otherwise, set **Internet Connection** to **Indirectly**.

Click **Advanced**. Then set DLAN performance parameters, enable broadcast and multicast, and set the maximum number of VPN connections and whether to transmit broadcast and multicast packets on VPN channels. See the figure below.

The image shows a configuration window with three sections: **VPN Performance**, **Broadcast**, and **Multicast**. In the **VPN Performance** section, the **Threads** value is set to 30. In the **Broadcast** section, the **Enable** checkbox is unchecked, **Start Port** is 1, and **End Port** is 10000. In the **Multicast** section, the **Enabled** checkbox is unchecked. At the bottom are **OK** and **Cancel** buttons.

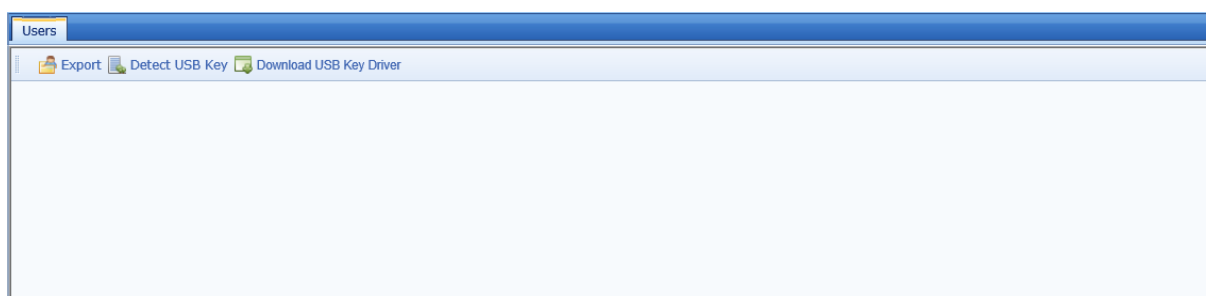
Threads: maximum number of VPN connections of the control device. The default value is **300**. A maximum of 1280 VPN connections are supported. Change the value of **Threads** under the guidance of SANGFOR technical support engineers when necessary.

Broadcast: whether to transmit broadcast packets on VPN channels. Only broadcast packets within the specified port range can be transmitted to avoid broadcast storms.

Multicast: whether to transmit multicast packets on VPN channels.

Local Users

On the **Local Users** page, you can manage VPN access accounts. That is, set the user name and password for accessing the VPN, whether to enable hardware binding authentication or DKEY authentication, whether to use virtual IP addresses, the encryption algorithm used for user accounts, account validity period, and internal permission of user accounts. You can also group users and set the public attributes of the group members. See the figure below.



Click **Detect USB Key** to detect whether a USB key is inserted into the computer that is currently logged in to the gateway console. If no DKey driver is installed, a prompt is displayed asking whether to download it. You can click **Download USB Key Driver** to download and install the DKey driver.



The DKey drive must be installed before the DKey is generated. Otherwise, the computer cannot identify the DKey hardware. To avoid DKey drive installation failure caused by program conflicts, exit programs including third-party anti-virus software and firewall before the installation.

Click **Delete** to delete selected users.

Click **Import From LDAP Server** to import user information from the domain server.



Before importing user information from the domain server, choose **VPN > Advanced > LDAP Server** and set the information about the LDAP server.

Click **Import From Text** to import user information from a TXT or CSV file.

Click **Export** to export user information from the equipment to a local computer. You can choose to export the user passwords in plaintext or cipher text mode. See the figure below.

A dialog box titled "Password Type" with two radio buttons: "Plaintext" (selected) and "Ciphertext". At the bottom are "Export" and "Cancel" buttons.

Click **New Group** and set the group name, group description, and public attributes of group members. See the figure below.

A dialog box titled "New Group" with the following fields: "Name:" (text input), "Description:" (text area), "Algorithm:" (dropdown menu showing "AES"), and a checkbox labeled "Enable My Network Places". At the bottom are "LAN Service", "Advanced", "OK", and "Cancel" buttons.

Click **Advanced** to set the VPN routing policy, multicast service and tunnel parameters.

Click **New User** and set the user name, password, description, and algorithm in sequence. See the figure below.

The screenshot shows a 'New User' configuration window. It is divided into several sections. The top section contains fields for Username, Password, Confirm Password, and Description. To the right of these are dropdown menus for Authentication (set to 'Local'), Algorithm (set to 'AES'), User Type (set to 'Mobile user'), and Added To (set to 'Default group'). There is also an 'Inherit group attributes' checkbox. The second section contains checkboxes for 'Hardware authentication', 'Enable USB key', and 'Assign virtual IP' (which is checked). To the right are fields for 'Certificate', 'USB Key', and 'IP Address' (set to '0.0.0.0'). The third section has a 'Valid Time' dropdown (set to 'All day'), an 'Enable expiration' checkbox, and an 'Expired At' field (set to '0-00-00'). The fourth section contains a grid of checkboxes: 'Enable user' (checked), 'Deny Internet access after login', 'Enable My Network Places' (checked), 'Enable multi-user login', 'Enable compression' (checked), and 'Deny password change online'. At the bottom of the window are four buttons: 'LAN Service', 'Advanced', 'OK', and 'Cancel'.

Authentication: user authentication type. You can choose local authentication (hardware authentication), LDAP authentication, and Radius authentication.

User Type: type of the VPN user that uses this account. It can be set to **Mobile user** or **Branch user**.

Inherit group attributes: whether to group users. If this check box is selected, the **Added to** parameter becomes active. You can add the user to a user group and apply the public attributes of this user group.



Before selecting the Inherit group attributes check box, add a user group. After a user is added to a user group, the Algorithm, Enable My Network Places, and LAN Service parameters of this user cannot be configured.

Hardware authentication: whether to enable hardware-based certificate authentication. After enabling hardware authentication, select the corresponding certificate file (*.id).

Enable USB key: whether to enable DKey authentication for mobile users. After DKey authentication is enabled, insert the DKey into a USB port on the computer and then click **USB Key**.

Assign virtual IP: used for the access of mobile clients. The **Assign virtual IP** check box must be selected for a mobile user. After this check box is selected, set a virtual internal IP address (in the virtual IP address pool) for this user. After this user is connected, the preset IP address is used as the virtual internal IP address. If the virtual IP address is set to 0.0.0.0, the system automatically assigns an internal IP address to this user from the virtual IP

address pool.



Before selecting the Assign virtual IP check box, choose VPN > Virtual IP Pool and set the virtual IP address pool.

Valid Time and **Enable expiration** are used to set the validity period and expiration time of the added user account.

If the VPN user needs to use the My Network Places service, select the **Enable My Network Places** check box.

Enable compression is used to set whether to compress the data transmitted between the gateway and the user by using the compression algorithm.



This setting is the unique technology of SANGFOR VPN. This improves the bandwidth usage and expedites data transmission. However, it is not applicable to all network environments. You need to set this item based on actual conditions in practice.

The **Deny Internet access after login** item is valid only for mobile users. If this check box is selected, a mobile user can access the internal network only through the VPN after the user is connected to the VPN. That is, the user cannot access the Internet.

The **Enable multi-user login** item sets whether to allow multiple users to share the account to log in to the VPN concurrently.

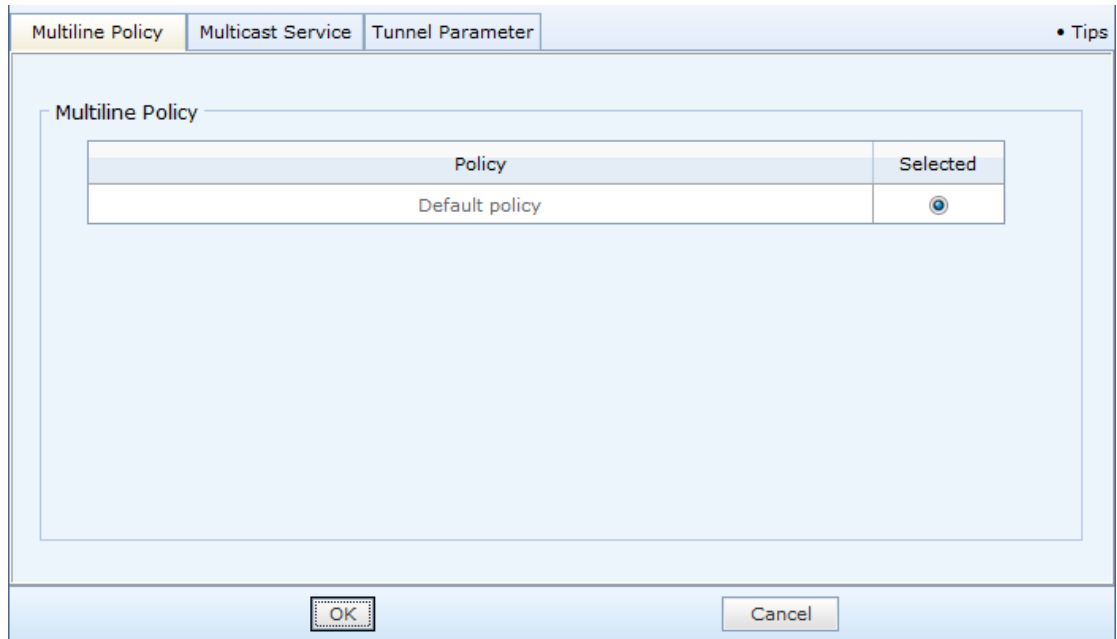
The **Deny password change online** item sets whether a mobile user can modify the login password after connected to the VPN. If this check box is not selected, the mobile user can modify the login password.

The **LAN Service** button is used to set the access permission of the user after connected to the VPN. That is, it is used to restrict the user to certain services. By default, it is not selected.

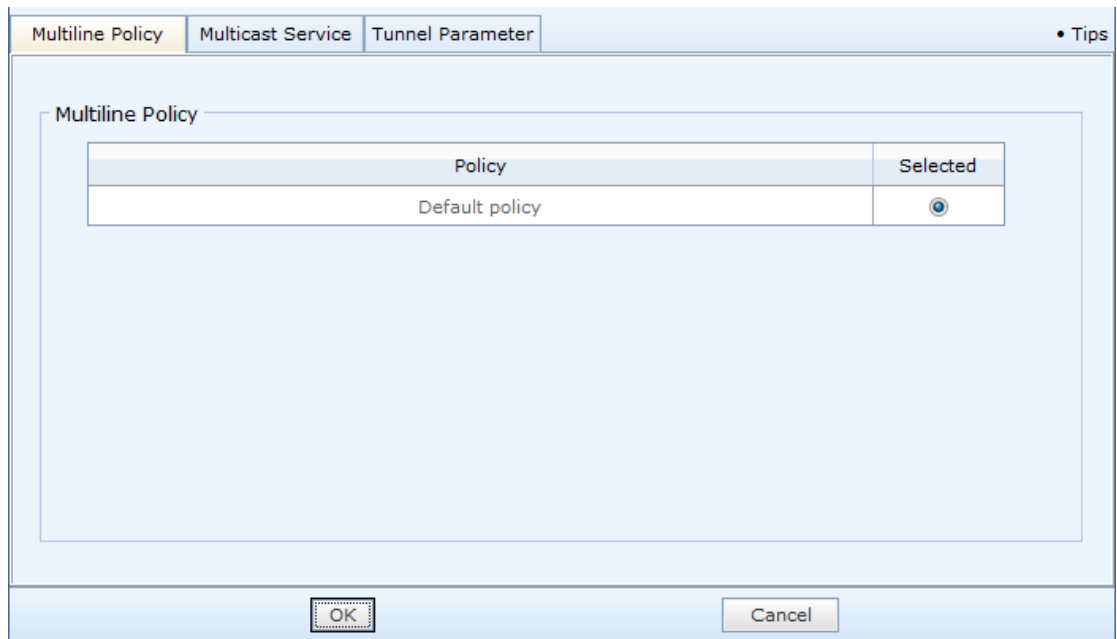


Before clicking LAN Service, choose VPN > Advanced > LAN Service and add required services.

The **Advanced** button is used to set advanced attributes of the user after the user is connected to the VPN. The advanced attributes include the routing policy, multicast service, tunnel parameters, and tunnel NAT. The routing policy indicates selecting different routes for different access users. The multicast service aims to meet the requirements of applications between the headquarters and branches that need multicast support. Intra-tunnel traffic control aims to avoid the case that the VPN traffic of a connected user is too heavy. Intra-tunnel NAT aims to resolve address conflicts resulted when two branches with the same internal network segment access the headquarters. The advanced setting page for mobile users is shown below.

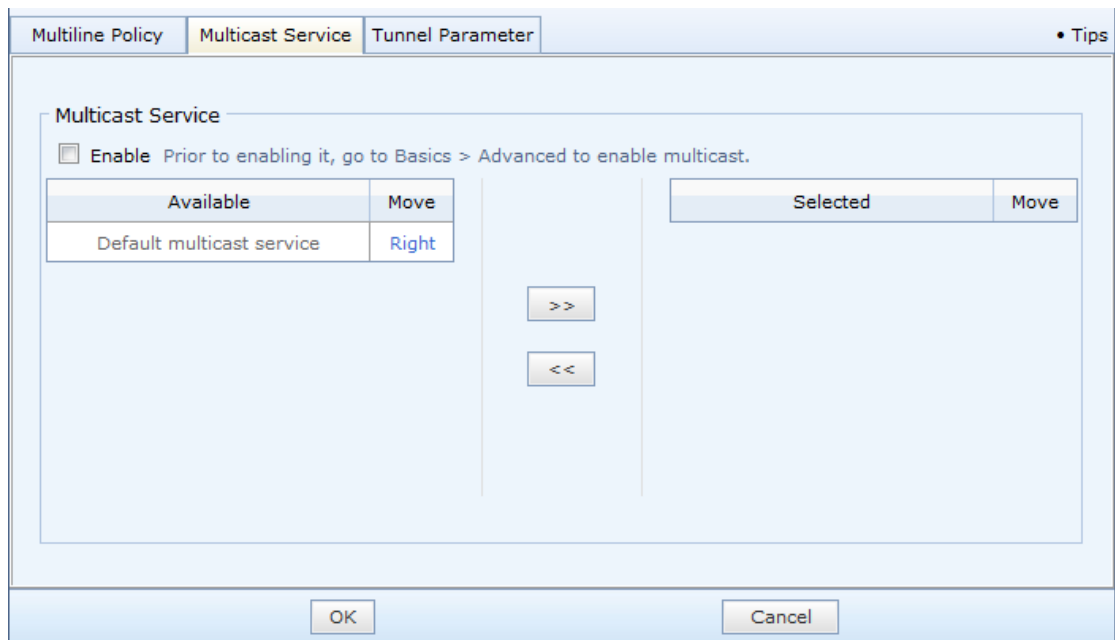


The advanced setting page for branch users is shown below.

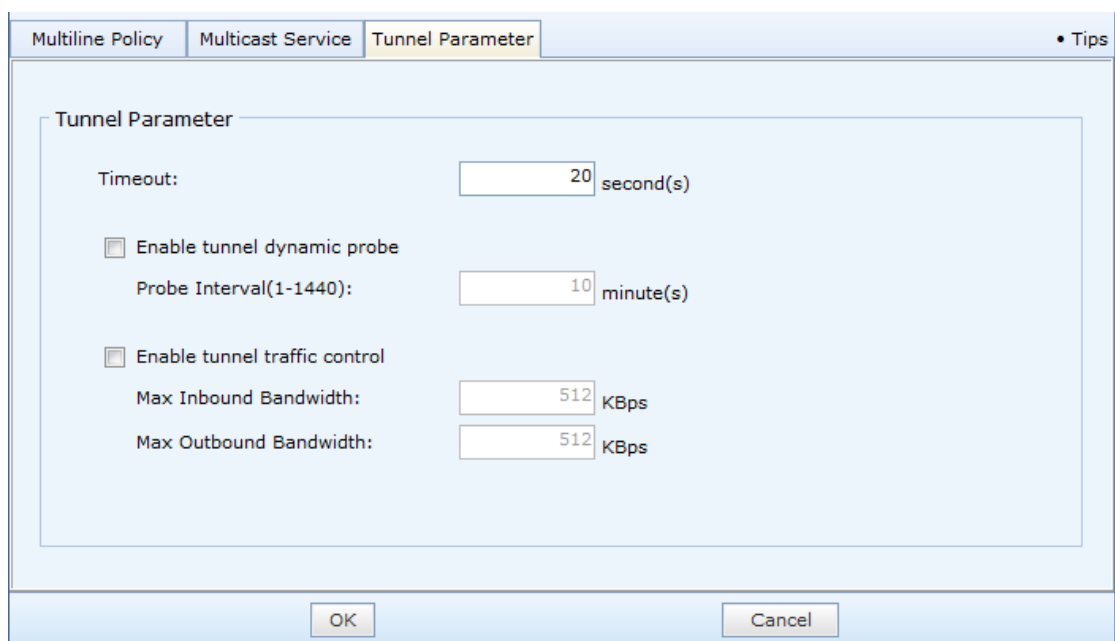


For details about setting the routing policy, see section 3.3.9.

For details about setting the multicast service, see section 3.3.14.2. The page is shown in the figure below.



The **Tunnel Parameter** tab page displays information including tunnel timeout time, dynamic tunnel detection, and intra-tunnel traffic control. See the figure below.



Timeout: SANGFOR VPN supports setting a timeout time for a network with a long delay and high packet loss rate. The timeout time configured at the headquarters takes effect for all tunnels. The default timeout time is 20 seconds. The timeout time needs to be extended in a poor network environment.

Enable tunnel dynamic probe: This item is valid when the local end or peer end has multiple lines. The SANGFOR VPN equipment detects the delay and packet loss rate of each line and selects the optimal line for data transmission.

Enable tunnel traffic control: This item is used when multiple VPN branches or mobile users access the equipment. If a branch or mobile user uses up the bandwidth at the headquarters, the access speed of other branches or mobile users is thereby lowered. To resolve this problem, you can specify the inbound and outbound bandwidths for each user. This ensures a proper access speed for all users.



In the Enable tunnel traffic control pane, a bandwidth range instead of a specific bandwidth value is set. For example, if Max Inbound Bandwidth is set to 100 Kbps, the actual bandwidth ranges from 80 Kbps to 120 Kbps. That is, the actual bandwidth fluctuates slightly around 100 Kbps.

On the **Tunnel NAP** tab page, you can translate the internal network segment of a branch into an address on a network segment in the virtual IP address pool. See the figure below.

No.	Source Subnet	Translate to Subnet	Subnet Mask	Operation
-----	---------------	---------------------	-------------	-----------

For details about the virtual IP address pool, see section 3.3.6.

Click **New** and enter the original subnet segment, proxy subnet segment, and subnet mask. You can also choose to enable the equipment to automatically assign an IP network segment from the virtual IP address pool. See the figure below.

Source Subnet:

Subnet Mask:

Translate to Subnet:

Source Subnet: actual internal subnet segment of the branch.

Subnet Mask: actual internal subnet mask of the branch.

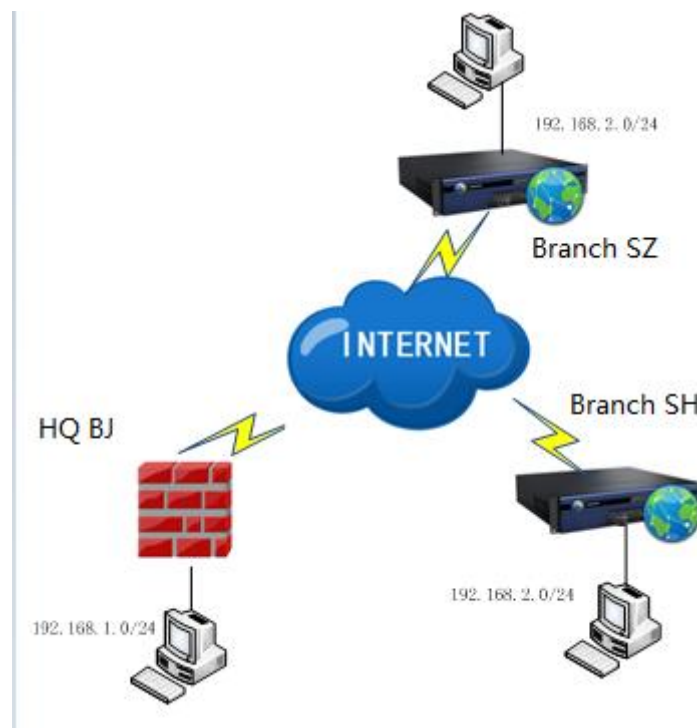
Translate to Subnet: virtual network segment after translation.



During configuration, ensure that the subnet mask must be matched. Tunnel NAT applies only to the network segment of the mask and the host ID does not change.

3.4.2.3.1 Tunnel NAT Case Study

The SANGFOR equipment in Beijing (headquarters) is deployed in routing mode. Shanghai branch (192.168.2.0/24) and Shenzhen branch (192.168.2.0/24) need to connect to the headquarters through the VPN. Tunnel NAT needs to be enabled on the SANGFOR equipment deployed in Beijing to resolve internal network segment conflicts between Shanghai branch and Shenzhen branch. The procedure for enabling tunnel NAT is as follows:



1. In the virtual IP address pool, add a virtual IP network segment 192.168.20.0/24. See the figure below.

Assigned To: Branch user ▼
 Branch VPN users who use tunnel NAT

Start IP:

End IP: Click Get or OK button Get

Subnet Mask:

Subnets: 1 ▼

OK Cancel

- On the **Local Users** page, add a branch account. Click **Advanced** and access the **Tunnel NAT** tab page. Select the **Enable** check box, click **New** to add a network segment 192.168.20.0/24 and associate this network segment with the branch account. See the figure below.

Username: Authentication: Local ▼

Password: Algorithm: AES ▼

Confirm Password: User Type: Branch user ▼

Description: Added To: Default group ▼

☐ Inherit group attributes

☐ Hardware authentication Certificate:

☐ Enable USB key USB Key:

☐ Assign virtual IP IP Address:

Valid Time: All day ▼

☐ Enable expiration Expired At: : :

☒ Enable user ☐ Enable My Network Places ☒ Enable compression

☐ Deny Internet access after login ☐ Enable multi-user login ☐ Deny password change online

LAN Service Advanced OK Cancel

Multiline Policy Multicast Service Tunnel Parameter **Tunnel NAT** • Tips

Tunnel NAT

☐ Enable **New**

No.	Source Subnet	Translate to Subnet	Subnet Mask	Operation

OK Cancel

Source Subnet:

Subnet Mask:

Translate to Subnet:

Auto Assign

OK Cancel

Click **OK** to apply the rule. Shenzhen branch can access the headquarters without modifying the internal IP address. The headquarters can access the services provided by the internal network of Shenzhen branch by using an IP address on the network segment 192.168.20.0/24.



Before using the multicast services in Advanced, choose VPN > Advanced > Multicast and add required services.

Before using tunnel NAT in Advanced, choose VPN > Virtual IP Pool and add the required branch virtual IP network segment.



Shenzhen branch and Shanghai branch cannot visit each other through an inter-tunnel route. If Shenzhen branch and Shanghai branch need to visit each other through the inter-tunnel route, tunnel NAT

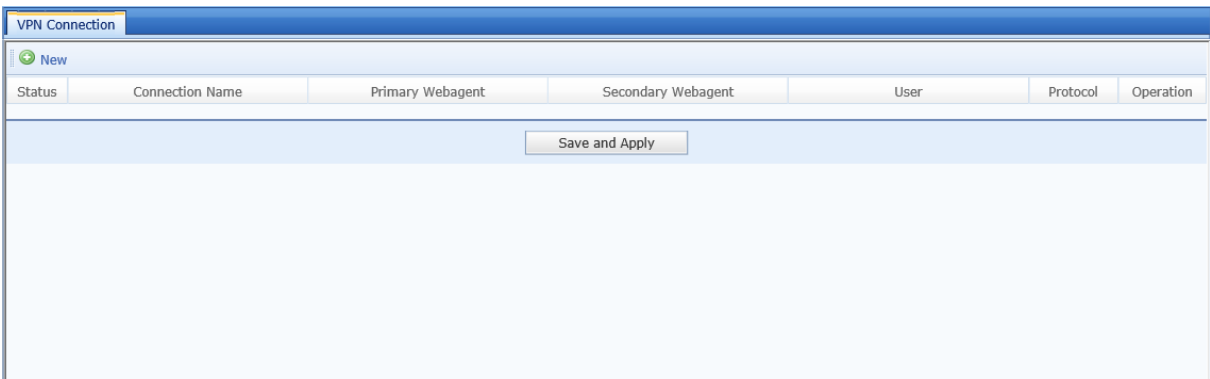
needs to be enabled for both of them for the purpose of translating their respective network segments into two different IP network segments. Then add an inter-tunnel route, of which the source is an actual physical IP network segment and the destination is a virtual IP network segment.

VPN Connection

The equipment provides the network node interconnection and setup functions to implement interconnection between multiple network nodes. You can perform setup on the **VPN Connection** page.



VPN connection needs to be enabled only when the equipment serves as a branch and needs to connect to other equipment at the headquarters. VPN connection does not need to be enabled if the local end is the equipment at the headquarters.



Click **New** to add a connection to the headquarters. See the figure below.

Connection Name:

Description:

Primary WebAgent:

Secondary WebAgent:

Shared Key:

Confirm Key:

Transfer Protocol:

Username:

Password:

Confirm Password:

☐ Cross-ISP Access Opt.

Packet loss rate: %

☒ Enable connection

Connection Name: name of the connection to the headquarters.

Description: description of the connection.

Primary WebAgent/Secondary WebAgent: Web agent to be connected to the headquarters. You can click **Test** to test whether the Web agent works properly. The test results are shown below.

Testing completed.

Primary WebAgent Secondary WebAgent



Test requests are initiated from the local end instead of the NGAF equipment. If the Web agent is represented by using a domain name and the test succeeds, the Webpage exists; otherwise, the Webpage does not exist. If the Web agent is presented by using a fixed IP address and the test succeeds, the IP address format is correct. The connection to the VPN may fail even if the test succeeds.

Transfer Protocol: protocol used for transmitting VPN packets. It can be set to **TCP** or **UDP**. The default value is

UDP.

Set **Shared Key**, **Username** and **Password** based on the account information provided by the headquarters.

The **Cross-ISP Access Opt.** item needs to be set when the headquarters and branches use different operators' lines for interworking and packet loss occurs frequently. This item can be set to **Low packet loss**, **High packet loss** or .



The **Cross-ISP Access Opt.** function needs to be enabled separately. Otherwise, it is invalid. If this function is enabled at the headquarters, all mobile users connected to the headquarters can use this function directly. Other branch hardware equipment connected to the headquarters also needs to enable this function.

Click **LAN Service** to set the permission of the peer end of the VPN connection. That is, specify the services that the peer end can access. Click **Enable connection** to activate the connection. Click **OK** to save the settings.

Available	Move
All ICMP Services	Right
All Services	Right
All TCP Services	Right
All UDP Services	Right

Selected	Allow	Deny	Schedule	Move
----------	-------	------	----------	------

>> <<

Default Action:

☒ Allow ☐ Deny

OK Cancel

Virtual IP Pool

If the SANGFOR VPN equipment assigns an idle IP address segment as the virtual IP address of mobile users, or assigns any IP network segment as the virtual IP network segment of branches, the virtual IP address pool is required to resolve IP address conflicts resulted when two branches with the same network segment concurrently access the headquarters through the VPN. After a mobile user is connected, a virtual IP address is assigned to this user. The source IP address of all operations performed by this mobile user is the assigned virtual IP address. You can specify network attributes for the connected mobile user in **Advanced**.

The procedure for configuring a virtual IP address is as follows:

1. Create a virtual IP address pool. The IP addresses in the virtual IP address pool are idle IP addresses on the LAN where the SANGFOR equipment resides.
2. Configure a mobile user to use a virtual IP address. If the virtual IP address is set to 0.0.0.0, a virtual IP address will automatically be assigned to this mobile user. After this mobile user is connected, the SANGFOR

equipment at the headquarters specifies a virtual IP address for the mobile user or selects an idle IP address from the virtual IP address pool and assigns it to the mobile user.

IP Range	Subnet Mask	Subnets	Assigned To	Operation
----------	-------------	---------	-------------	-----------

Save and Apply

Click **New**. In the **Virtual IP Pool** dialog box, set the start IP address. See the figure below.

Assigned To: Mobile user ▼
The mobile VPN users

Start IP:

End IP:

OK Cancel

Click **Advanced** on the **Virtual IP Pool** page and set the virtual IP subnet mask, DNS, and WINS, which are to be assigned to the virtual network adapter of the mobile client. See the figure below.

Preferred DNS:

Alternate DNS:

Preferred WINS:

Alternate WINS:

Subnet Mask:

OK Cancel



After setting the advanced options on the Virtual IP Pool page, the virtual network adapter (SANGFOR VPN virtual network adapter) on the mobile client must be set to automatically obtain IP address and DNS. Otherwise, the information specified by the advanced options will not be assigned to the virtual network adapter of the mobile client.

3. Create a branch virtual IP address pool. When a branch accesses the headquarters, the original network segment of the branch is replaced by a network segment in the virtual IP address pool. This is to resolve internal IP address conflicts resulted when two branches with the same network segment concurrently accesses the headquarters. Set the start IP address, subnet mask, and network segment quantity. Then click **Get** and the end IP address is automatically calculated. See the figure below.

Assigned To: Branch user ▼
Branch VPN users who use tunnel NAT

Start IP: 192.168.20.1

End IP: 192.168.20.255 **Get**

Subnet Mask: 255.255.255.0

Subnets: 1 ▼

OK Cancel

Start IP: the first IP address on the branch virtual IP address segment.

End IP: the last IP address on the branch virtual IP address segment.

Get: to calculate the last IP address on the virtual IP address segment automatically.

Subnets: number of virtual IP address segments.

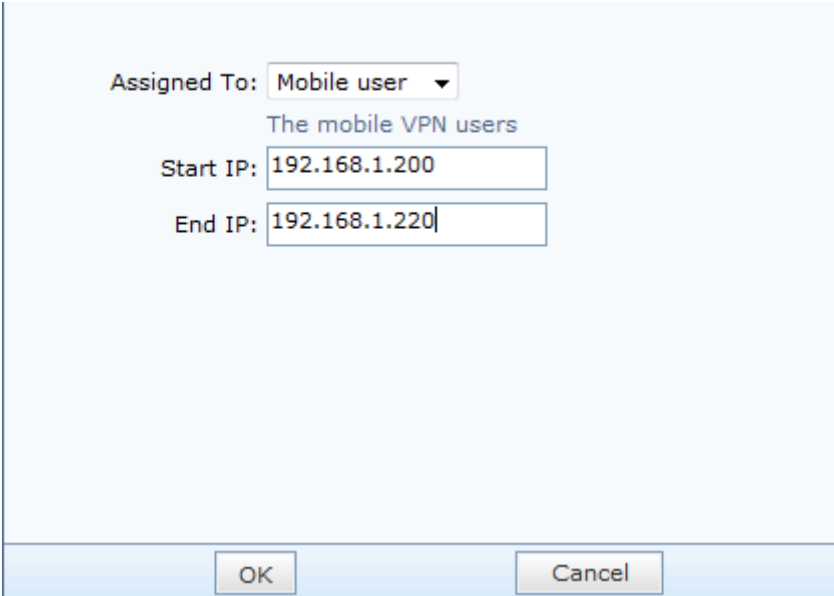
Subnet Mask: subnet mask of the virtual IP address segment. It is the same as the internal subnet mask of the branch.

After setting the branch virtual IP address segment, choose **VPN > Local Users** and create a user. Set **Type** to **Branch user**. Click **Advanced** and configure the branch network segment to be transited on the **Tunnel NAT** tab page.

1.1.1.1.1. Case Study

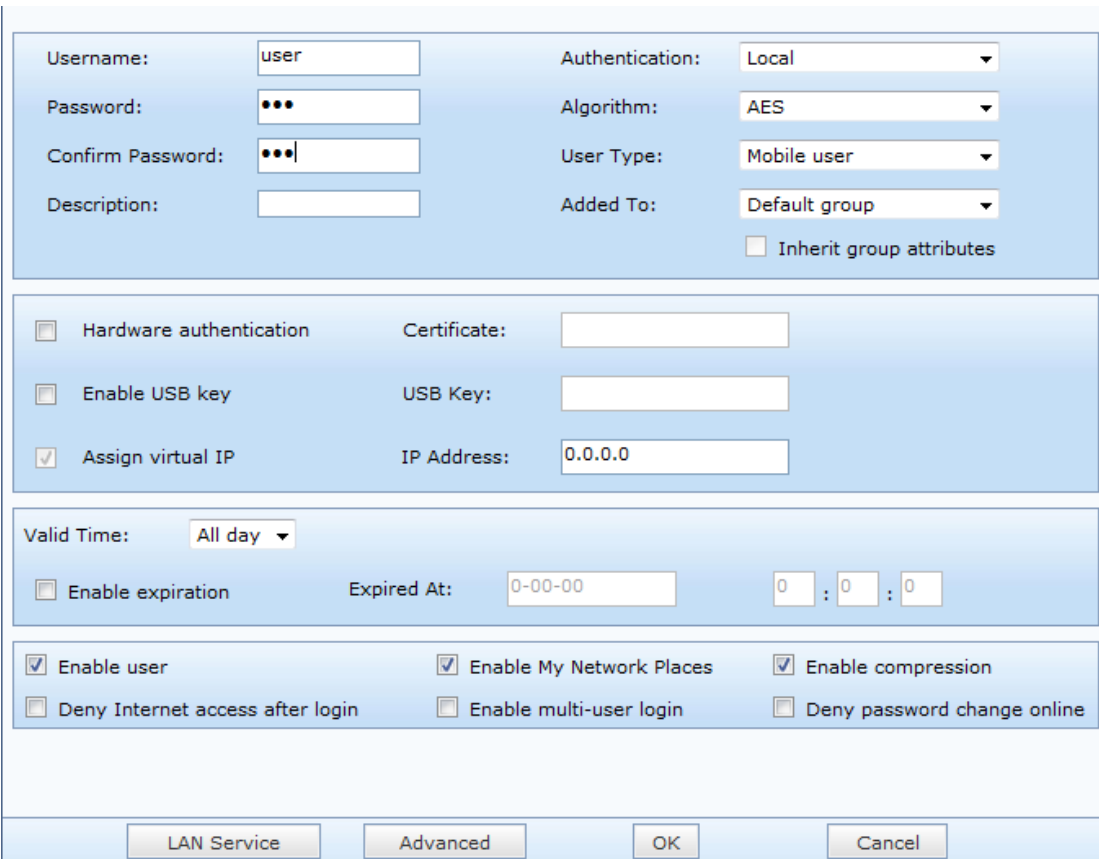
The SANGFOR equipment is deployed in routing mode at the headquarters. Remote mobile users need to access the headquarters through the VPN. The configuration procedure is as follows:

Add a rule in **Virtual IP Pool**. Set an IP address segment that is on the same network segment as the LAN interface of the equipment and not used by internal users. See the figure below.



The screenshot shows a configuration window for a Virtual IP Pool. It has a light blue background. At the top, there is a label "Assigned To:" followed by a dropdown menu showing "Mobile user". Below this, there is a link "The mobile VPN users". Then, there are two input fields: "Start IP:" with the value "192.168.1.200" and "End IP:" with the value "192.168.1.220". At the bottom, there are two buttons: "OK" and "Cancel".

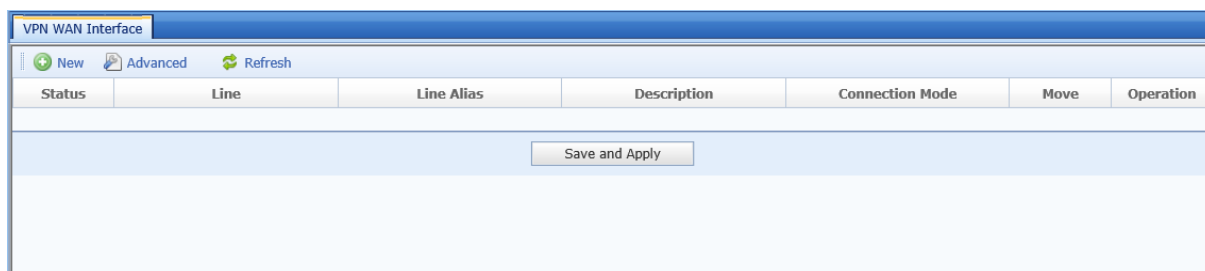
On the **Local Users** page, click **New User** to add a new and set **User Type** to **Mobile user**. The default value of **IP Address** is **0.0.0.0**, which means that a virtual IP address will be automatically assigned to the user. You can also manually specify a virtual IP address for the user.



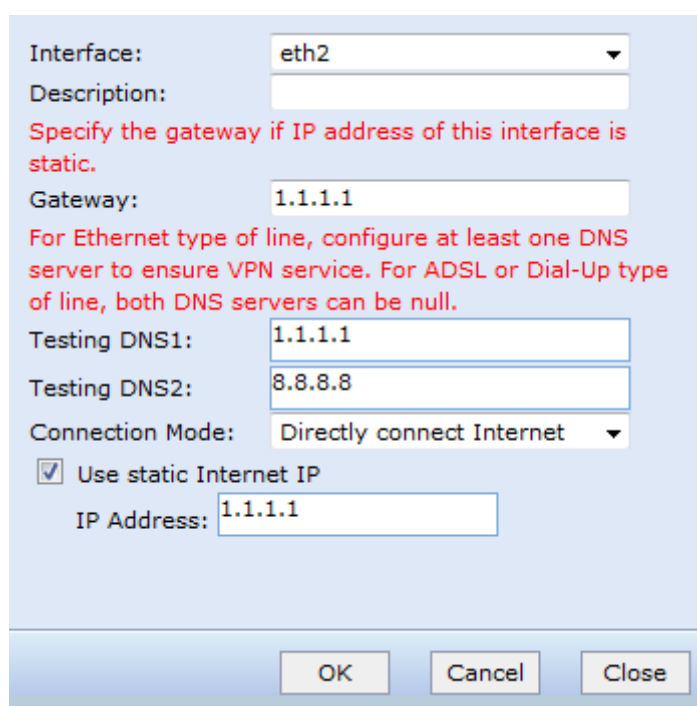
The screenshot shows a complex configuration page for a Local User. It has a light blue background and is divided into several sections. The top section contains fields for "Username:" (value: "user"), "Password:" (masked with "•••"), "Confirm Password:" (masked with "•••"), "Description:" (empty), "Authentication:" (dropdown: "Local"), "Algorithm:" (dropdown: "AES"), "User Type:" (dropdown: "Mobile user"), and "Added To:" (dropdown: "Default group"). There is also an unchecked checkbox "Inherit group attributes". The middle section contains three rows of options: "Hardware authentication" (unchecked), "Enable USB key" (unchecked), and "Assign virtual IP" (checked). Each row has a corresponding field: "Certificate:" (empty), "USB Key:" (empty), and "IP Address:" (value: "0.0.0.0"). The bottom section contains "Valid Time:" (dropdown: "All day") and an unchecked checkbox "Enable expiration". Below this is a row of three time input fields: "Expired At:" (value: "0-00-00"), and two empty fields for "0", "0", and "0" separated by colons. At the very bottom, there are six checkboxes: "Enable user" (checked), "Deny Internet access after login" (unchecked), "Enable My Network Places" (checked), "Enable multi-user login" (unchecked), "Enable compression" (checked), and "Deny password change online" (unchecked). At the bottom of the page, there are four buttons: "LAN Service", "Advanced", "OK", and "Cancel".

VPN WAN Interface

On the **VPN WAN Interface** page, you can define external VPN interfaces. See the figure below.



Click **Add** to add an external interface, as shown in the figure below.



Interface: external VPN interface. Only WAN route interfaces can be configured as external VPN interfaces.

Gateway: gateway address corresponding to the external interface. This parameter needs to be set only when the interface type is static IP address, and does not need to be set when the interface type is ADSL or DHCP.

Testing DNS: DNS address provided by the operator. This parameter does not need to be set if the interface type is set to ADSL.

Connection Mode: Internet connection mode. It can be set to **Directly connect Internet** or **Indirectly connect Internet**. If the interface connects to the Internet directly, set this parameter to **Directly connect Internet**.

Use static Internet IP: static public network IP address assigned to the interface.

Click  to perform DNS detection setup. See the figure below.



1. Only WAN physical route interfaces can be configured as external VPN interfaces.
2. Multiple external VPN interfaces can be configured for implementing multiline routing of the VPN.

VPN LAN Interface

On the **VPN LAN Interface** page, you can define internal VPN interfaces. See the figure below.

Click **New** and select an internal VPN interface, as shown in the figure below.

Only a non-WAN interface with a static IP address can be configured as an internal VPN interface.

VPN Interface IP: IP address of the virtual network adapter for VPN services.



The **Assigned automatically** option button is selected by default and you are advised to retain the default setting. If a prompt indicating IP address conflicts is displayed, select **Specified** and set the IP address and subnet mask.



VPN interfaces are virtual interfaces of the SANGFOR gateway. They are not physical interfaces.

Multiline Policy

The SANGFOR equipment provides a powerful VPN multiline policy where different primary and secondary line groups can be selected based on the conditions of the external lines between the local end and peer end. Traffic can be evenly distributed by session or packet. See the figure below.

Name	Request Assignment	Description	Operation
Default policy	Assign sessions evenly	Default policy	Edit

Save and Apply

Click **New**. The multiline policy editing dialog box shown below is displayed.

Basic Settings

Name:

Description:

Line Settings

Local Lines Peer Lines Threshold for VPN-Data-Transfer Line Selection ms

Primary Lines

Local Line	Peer Line	Move
Line 1	Line 1	Right
Line 1	Line 2	Right
Line 1	Line 3	Right
Line 1	Line 4	Right

Secondary Lines

Local Line	Peer Line	Move
------------	-----------	------

Request Assignment

☒ Assign sessions evenly ☐ Assign packets evenly

OK Cancel

Name: name of the policy.

Line Settings: You can set the number of external lines of the local end, number of lines of the peer end, and threshold for line selection.

Primary Lines: primary line groups for VPN connections. You can click **Right** in the **Move** column to move a selected line group to **Secondary Lines**.

Secondary Lines: secondary line groups for VPN connections.

Request Assignment: It can be set to **Assign sessions evenly** or **Assign packets evenly**.



After the multiline policy is set, you need to enable it in **Advanced of Local Users**.

Local Subnet

When the internal network at the headquarters consists of multiple subnets, a local subnet list needs to be configured if mutual access is required between other VPN users and the subnets of the internal network at the headquarters. For example, the internal network at the headquarters consists of two subnets, 192.200.100.x and 192.200.200.x. You can configure a local subnet list to implement mutual access between the network segments of branch users, mobile users, and the headquarters. The procedure is as follows:

1. On the **Local Subnet** page, configure the subnets to be interconnected. See the figure below.

No.	IP Address	Subnet Mask	Operation
-----	------------	-------------	-----------

Click **New** to add a local subnet. See the figure below.

IP Address:

Subnet Mask:

OK

Set **IP Address** and **Subnet Mask** to the network ID and subnet mask on a non-direct network segment of the VPN equipment in the internal network at the headquarters.

2. Set routes for the subnets to be interconnected in **Static Route**. For details, choose **Network > Routing > Static Route**.



The local subnet list is like a declaration. The network segments defined on the **Local Subnet** page are considered as VPN network segments by the VPN equipment and software clients. After passing through the VPN equipment or software, all packets destined for these network segments are encapsulated and transmitted on the VPN tunnel. Generally, after adding subnet segments on the **Local Subnet** page, you need to configure static routes to implement access to multiple subnets.

Tunnel Route

The SANGFOR equipment provides powerful VPN tunnel routing functions. After tunnel routes are configured, interconnection between VPNs (software/hardware) can be easily implemented. See the figure below.

Status	Source	Src Subnet Mask	Destination	Dst Subnet Mask	Destination Route User	Move	Operation
--------	--------	-----------------	-------------	-----------------	------------------------	------	-----------

1.1.1.1.2. Case Study

For example, the headquarters (Shenzhen 192.168.1.x/24) establishes connections with two branches Shanghai 172.16.1.x/24 and Guangzhou 10.1.1.x/24. Shanghai and Guangzhou branches interconnect with the headquarters through connection management configuration. There is no VPN connection between Shanghai branch and Guangzhou branch. You can set a tunnel route to implement mutual access between Shanghai and Guangzhou. The procedure is as follows:

1. On the **Tunnel Route** page of Shanghai branch, select **Enable tunnel route** and click **New** to add a route to Guangzhou branch. See the figure below.

Source IP: 172.16.1.0

Subnet Mask: 255.255.255.0

Destination IP: 10.1.1.0

Subnet Mask: 255.255.255.0

Dst Route User: SH

☒ Enabled

☐ Access Internet via destination route user

OK Cancel

Source IP: source IP address. It should be set to 172.16.1.0 in this example.

Subnet Mask: subnet mask of the source IP address. It should be set to 255.255.255.0 in this example.

Destination IP: destination IP address. It should be set to 10.1.1.0 in this example.

Subnet Mask: subnet mask of the destination IP address. It should be set to 255.255.255.0 in this example.

Dst Route User: VPN user that the route directs to. In this example, set it to the user that establishes the VPN connection between Shanghai branch and Shenzhen branch.



Source IP and Destination IP specify the source IP address and destination IP address of data. If the data transmitted on the VPN tunnel match the settings, the route settings take effect and data is forwarded to the corresponding VPN equipment. **Dst Route User** specifies the VPN equipment to which the data is to be routed. In this example, Shanghai branch establishes a VPN connection with the headquarters by using the user name Shenzhen-Shanghai in VPN Connection. Therefore, the data forwarded to the headquarters is labeled Shenzhen-Shanghai.

2. On the **Tunnel Route** page of Guangzhou branch, select **Enable tunnel route** and click **New** to add a route to Shanghai branch. See the figure below.

Source IP: 10.1.1.0

Subnet Mask: 255.255.255.0

Destination IP: 172.16.1.0

Subnet Mask: 255.255.255.0

Dst Route User: GZ ▼

☒ Enabled

☐ Access Internet via destination route user

OK Cancel

Source IP: source IP address. It should be set to 10.1.1.0 in this example.

Subnet Mask: subnet mask of the source IP address. It should be set to 255.255.255.0 in this example.

Destination IP: destination IP address. It should be set to 172.16.1.0 in this example.

Subnet Mask: subnet mask of the destination IP address. It should be set to 255.255.255.0 in this example.

Dst Route User: VPN user that the route directs to. In this example, set it to the user that establishes the VPN connection between Guangzhou branch and Shenzhen branch.

The network access data in a branch can be forwarded to the headquarters through a tunnel route and network access is performed through the public network interfaces at the headquarters. For example, set Shanghai branch to access the Internet through the headquarters. See the figure below.

Source IP:	172.16.1.0
Subnet Mask:	255.255.255.0
Destination IP:	0.0.0.0
Subnet Mask:	0.0.0.0
Dst Route User:	SH
<input checked="" type="checkbox"/> Enabled	
<input checked="" type="checkbox"/> Access Internet via destination route user	
<div>OK Cancel</div>	

Source IP: source IP address. Set it to the IP address that needs to access the Internet through the headquarters.

Subnet Mask: subnet mask of the source IP address. It should be set to 255.255.255.0 in this example.

Dst Route User: VPN user that the route directs to.

Select **Access Internet via destination route user** to apply the settings.



1. In the case of network access through lines at the headquarters, choose **Firewall > Address Translation > Source Address Translation** on the equipment at the headquarters and add source address translation rules for VPN network segments. For details, see the configuration description of the firewall.
2. If the NGAF equipment serves as the headquarters and branches need to access the Internet through the headquarters, perform operations under the guidance of SANGFOR technical support engineers.

IPSec VPN

The SANGFOR equipment supports interworking with third-party VPN equipment by establishing standard IPSec VPN connections.

1.1.1.1.3. Phase I

On the **Phase I** page, you can set information about the peer VPN equipment that needs to establish a standard IPSec connection with the SANGFOR gateway. This is phase I of the IPSec negotiation. See the figure below.

Status	Device Name	Device Address	Authentication Type	Connection Mode	ISAKMP Lifetime(s)	Description	Operation
OK							

Select **Outlet Line** and click **New**. The dialog box shown in the figure below is displayed.

Device Name:

Description:

Address Type:

Static IP:

Authentication Method

Pre-Shared Key:

Confirm Key:

☒ Enable this device

☒ Auto connect

Advanced OK Cancel

Click **Advanced**. In the displayed **Advanced** dialog box, set advanced options. See the figure below.

ISAKMP Lifetime: (s)

Retry Times:

Mode:

D-H Group:

ISAKMP Algorithm List

Authentication Algorithm:

Encryption Algorithm:

1.1.1.1.4. Phase II

On the **Phase II** page, you can set parameters of phase II of the IPSec negotiation. See the figure below.

Phase II

Inbound Policy

Status	Policy Name	Source IP	Peer Device	Inbound Service	Description	Operation
<input type="button" value="New"/>						

Outbound Policy

Status	Policy Name	Source IP	Peer Device	Outbound Service	Security Option	Description	Operation
<input type="button" value="New"/>							

In the **Inbound Policy** pane, set the policy for routing packets sent from the peer end to the local end. Click **New**. The dialog box for adding a policy is displayed. See the figure below.

Policy Name:	<input type="text" value="pix"/>
Description:	<input type="text"/>
Source:	<input type="text" value="Subnet"/>
Subnet:	<input type="text" value="192.100.0.0"/>
Mask:	<input type="text" value="255.255.255.0"/>
Peer Device:	<input type="text"/>
Inbound Service:	<input type="text" value="All Services"/>
Schedule:	<input type="text" value="All day"/>
<input checked="" type="radio"/> Allow in the above schedule <input type="radio"/> Deny in the above schedule <input type="checkbox"/> Enable Expiry Time Expiry Time: <input type="text" value="0-00-00"/> <input type="text" value="0"/> : <input type="text" value="0"/> : <input type="text" value="0"/> <input checked="" type="checkbox"/> Enable This Policy	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

In the **Outbound Policy** pane, set the policy for routing packets sent from the local end to the peer end. Click **New**. The dialog box for adding a policy is displayed. See the figure below.

Policy Name:

Description:

Source:

Subnet:

Mask:

Peer Device:

SA Lifetime: seconds

Outbound Service:

Security Option:

Schedule:

☒ Allow in the above schedule

☐ Deny in the above schedule

☐ Enable Expiry Time

Expiry Time: : :

☒ Enable This Policy

☒ Perfect Forward Security



The Inbound Service, Outbound Service, and Schedule options are extended by SANGFOR. These options are valid only on the local equipment. They are not included in negotiation in the process of establishing a VPN connection with the third-party equipment. The source IP address is the intersection of the source IP addresses set and local/peer device services.

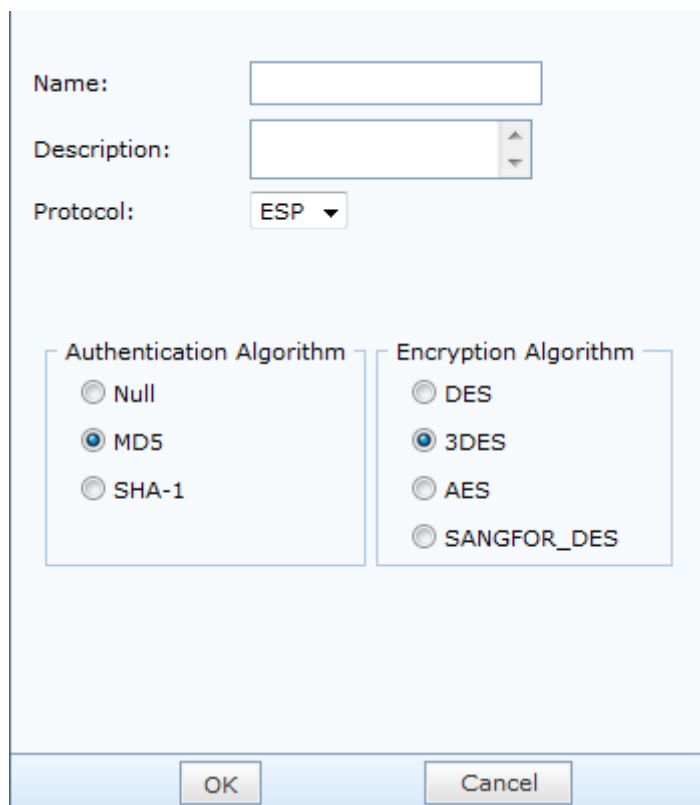
1.1.1.1.5. Security Options

On the **Security Options** page, you can set the parameters for establishing standard IPSec connections with the peer end. This is phase II of the standard IPSec negotiation. See the figure below.

Security Options					
New					
Name	Protocol	Authentication Algorithm	Encryption Algorithm	Description	Operation
Default security option	ESP	MD5	3DES		Edit

Before establishing an IPSec connection with the third-party equipment, understand the connection policy used by

the peer equipment, including the used protocol (AH or ESP), authentication algorithm (null, MD5 or SHA-1), and encryption algorithm (DES, 3DES, AES or SANGFOR_DES). Then click **New**. See the figure below.



The screenshot shows a configuration window for Security Options. It has a light blue background and a thin blue border. At the top, there are three fields: 'Name:' with an empty text box, 'Description:' with an empty text box and a small vertical scrollbar, and 'Protocol:' with a dropdown menu showing 'ESP'. Below these are two side-by-side panels. The left panel is titled 'Authentication Algorithm' and contains three radio buttons: 'Null', 'MD5' (which is selected), and 'SHA-1'. The right panel is titled 'Encryption Algorithm' and contains five radio buttons: 'DES', '3DES' (which is selected), 'AES', and 'SANGFOR_DES'. At the bottom of the window are two buttons: 'OK' and 'Cancel'.

The SANGFOR equipment establishes an IPSec connection with the peer end after negotiation based on the preset connection policy.



Encryption Algorithm specifies the data encryption algorithm used at phase II of the IPSec negotiation.

If the SANGFOR equipment needs to interconnect with multiple pieces of equipment that adopts different connection policies, you need to add these connection policies to the Security Options page.

Objects

The **Objects** configuration module contains two sub-modules: **Schedule** and **Algorithm**.

Schedule

On the **Schedule** page, you can define commonly used time segment combinations, which may be used in **Local Users** and **LAN Service**. The current time on the equipment prevails. See the figure below.

Name	Description	Operation
All day	All day	View

Save and Apply

Click **New**. The **Schedule** dialog box shown below is displayed.

Name: Working Hours

Description:

Click and drag over the grids to select time segment(s).

All	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon																								
Tue																								
Wen																								
Thu																								
Fri																								
Sat																								
Sun																								

Date: Mon - Sun

Time: 14:00 - 18:00

Select Deselect OK Cancel

In the preceding figure, a time segment named Working Hours is defined. By default, the rules are effective in all time segments. Select a time segment combination and click . Then the rules are ineffective in the selected time segment and effective in other time segments. Click **OK**. The rules are effective in the time segments marked in green and ineffective in the time segments marked in gray.

Algorithms

On the **Algorithms** page, you can view and add data encryption algorithms supported by the equipment. All data transmitted on the VPN is encrypted by using the specified algorithm to ensure data security. See the figure below.

Algorithm	Type	Provider	Description	Operation
DES	Encryption Algorithm	Walter tuchman and Carl Meyer	Data Encryption Standard for encrypt data	-
3DES	Encryption Algorithm	Walter tuchman and Carl Meyer	Triple-DES Standard for encrypt data	-
MD5	Authentication Algorithm	Ronald L. Rivest of the RSA	Message-Digest Algorithm for Authentication	-
AES	Encryption Algorithm	Joan Daemen and Vincent Rijmen	Advanced Encryption Standard for encrypt data	-
SHA-1	Authentication Algorithm	US National Security Agency (NSA)	Secure Hash Algorithm 1 for Authentication	Delete
SANGFOR_DES	Encryption Algorithm	Sangfor vpn group	Data Encryption Standard for encrypt data	Delete

Save and Apply

As shown in the preceding figure, multiple encryption algorithms and authentication algorithms including DES, 3DES, MD5, AES, SHA-1, SANGFOR_DES are set on the equipment. You can add other algorithms as required.

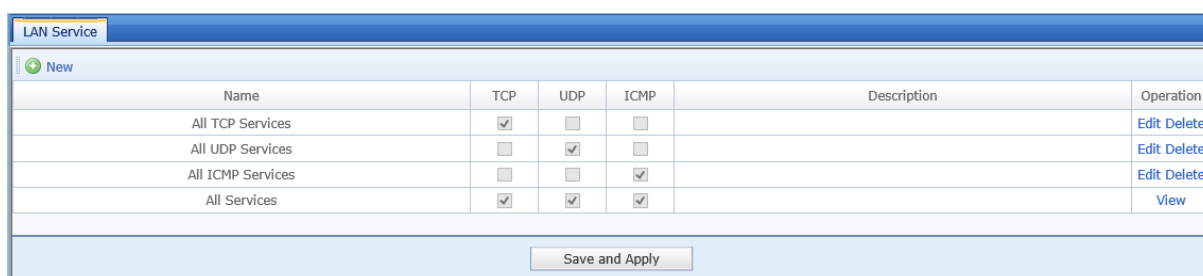
To add algorithms, contact SANGFOR.

Advanced

The **Advanced** configuration module consists of multiple sub-modules including **LAN Service**, **Multicast**, **LDAP Server**, **RADIUS Server**, **Dynamic Routing**, and **Certificate**.

LAN Service

The SANGFOR equipment can specify access permission for connected VPN users. It can restrict an IP address or mobile user on the internal network of a branch to specific services on a certain computer of the internal network. It can also set inbound and outbound policy parameters for interconnecting with third-party equipment. For example, the equipment allows user **test** to access Web services of the Web server at the headquarters and denies the access requests of user **test** to other services of the Web server. Or, it allows an IP address in the internal network of branch1 to access the SQL server at the headquarters and denies the access requests of other IP addresses in the internal network. Security management on the VPN tunnel can be implemented through service access authorization.



Name	TCP	UDP	ICMP	Description	Operation
All TCP Services	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		Edit Delete
All UDP Services	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Edit Delete
All ICMP Services	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Edit Delete
All Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		View

To set service access permission, you need to create LAN services and then grant permission to users. By default, the system does not restrict the access permission of VPN users.

3.4.13.1.1 Case Study

A customer requires that only the internal IP address 172.16.1.100 of a branch can access the FTP server 192.168.1.20 at the headquarters, and that the access requests initiated by other IP addresses and those initiated by 172.16.1.100 to other services are denied. The configuration procedure is as follows:

In **LAN Service**, click **New**. In the **LAN Service** dialog box, set **Name** and **Protocol**. Set **Protocol** to **TCP** in this example. See the figure below.

Name:

Description:

Protocol: ☒ TCP ☐ UDP ☐ ICMP

Source IP	Source Port	Destination IP	Destination Port	Operation
172.16.1.100-17...	1-65535	192.168.1.20-19...	20-21	Edit Delete

1. Click **New**. In the **IP Range** dialog box, set relevant parameters. See the figure below.

Source IP:

Start IP:

End IP:

Source Port: -

Destination IP:

Start IP:

End IP:

Destination Port: -

Source IP: Set it to the internal IP address 172.16.1.200.

Source Port: The value ranges from 1 to 65535.

Destination IP: Set it to the IP address of the FTP server 192.168.1.20.

Destination Port: Set it to the FTP service port 20-21.



After defining the LAN service, you need to grant internal network permission for the user in Local Users. The LAN service settings can also apply to the Inbound Service and Outbound Service parameters in Inbound Policy and Outbound Policy of IPSec VPN. For details, see the above sections.

2. In **Local Users**, click **Edit** in the line of user **Branch**. The page shown below is displayed.

The dialog box shows the configuration for user 'Branch'. It includes fields for Username, Password, Confirm Password, and Description. Authentication is set to 'Local', Algorithm to 'AES', User Type to 'Branch user', and Added To to 'Default group'. There is an unchecked checkbox for 'Inherit group attributes'. Below these are sections for hardware authentication (Certificate, USB Key, Assign virtual IP with IP Address 0.0.0.0), Valid Time (All day), and Enable expiration (Expired At: 0-00-00). At the bottom, there are checkboxes for 'Enable user' (checked), 'Deny Internet access after login' (unchecked), 'Enable My Network Places' (unchecked), 'Enable multi-user login' (unchecked), 'Enable compression' (checked), and 'Deny password change online' (unchecked). Buttons at the bottom include 'LAN Service', 'Advanced', 'OK', and 'Cancel'.

3. In the dialog box, move the Branch service to the service list on the right, select **Allow**. Then select **Deny** under **Default Action**. See the page below.

The dialog box is titled 'Select LAN Service'. It has two main sections. The first section, 'Select LAN Service', contains a table with 'Available' services and a 'Move' button. The 'Available' services are 'All TCP Services', 'All UDP Services', 'All ICMP Services', and 'All Services', each with a 'Right' button. There are '>>' and '<<' buttons between the two tables. The second table, 'Selected', contains 'Branch' with 'Allow' checked, 'Deny' unchecked, 'Schedule' set to 'All day', and a 'Move' button with 'Up Down Left' text. The second section, 'Default Action', has radio buttons for 'Allow' and 'Deny', with 'Deny' selected. Buttons at the bottom are 'OK' and 'Cancel'.

After the preceding settings are finished, the internal IP address 172.168.1.200 of Branch can access the FTP server 192.168.1.20 and the access requests initiated by other IP addresses are denied.



Other computers at the headquarters cannot access Branch either. When another computer at the headquarters initiates a request to access the branch, the destination IP address carried in the response packet sent by the computer at the branch is not 192.168.1.20, and therefore the packet is blocked.

Multicast Service

The SANGFOR supports the transmission of multicast services on tunnels to meet the needs of using applications like VoIP and video conference through the VPN. These applications require multicast support. You can define multicast services. The IP address range is 224.0.0.1-239.255.255.255 and the port range is 1-65535. See the figure below.

Name	Description	Operation
Default multicast service	Default multicast service	Edit

[New](#) [Save and Apply](#)

Click **New**. On the multicast service editing page, set the multicast address and port. See the figure below.

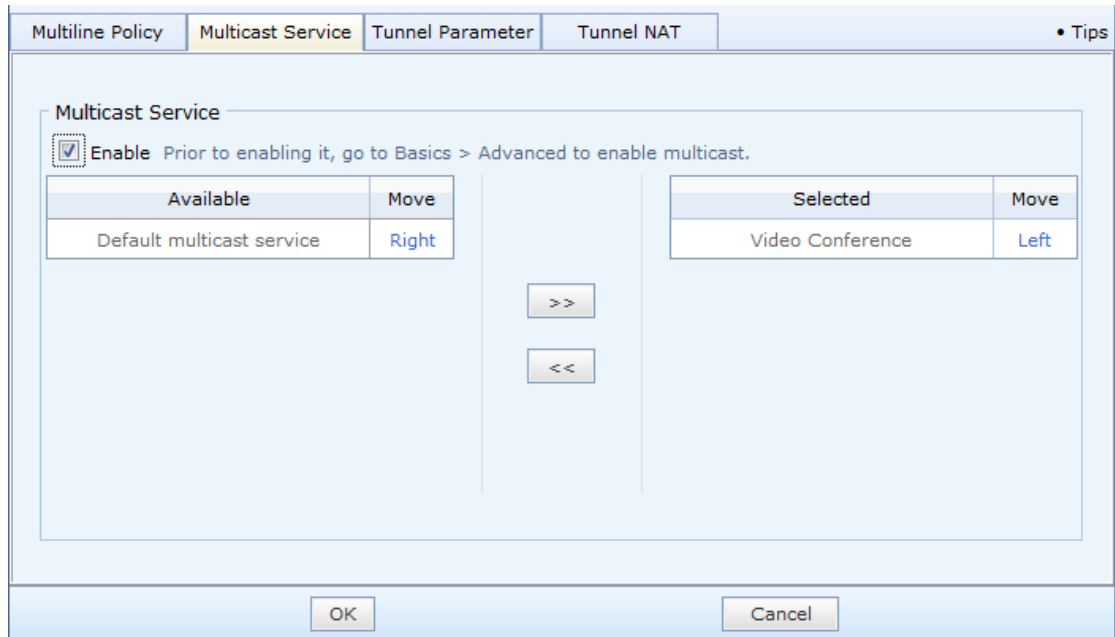
Name:

Description:

Start IP	End IP	Port	Description	Operation
226.5.6.7	226.5.6.7	20000-...		Edit Delete

[New](#) [OK](#) [Cancel](#)

After defining the multicast service, create a user in **Local Users**, choose **Advanced** > **Multicast** and configure the multicast service. See the figure below.



LDAP Server

The VPN service provided by the SANGFOR equipment supports third-party LDAP authentication. To enable third-party authentication, correctly set the information about the third-party LDAP server on the **LDAP Server** page, including the server IP address, port number, and administrator password. See the figure below.

Click **Advanced**. In the **Advanced LDAP Settings** dialog box, set LDAP information as required. See the figure below.

Server Type: Active Directory

User Filter: (Objectcategory=person)

User Attribute: sAMAccountName

Root DN: CN=users,DC=sinfors,DC=cc

Base DN: CN=users,DC=sinfors,DC=cc

Timeout(sec): 10

OK Cancel

RADIUS Server

The VPN service provided by the SANGFOR equipment supports third-party RADIUS authentication. To enable third-party authentication, correctly set the information about the third-party RADIUS server on the **RADIUS Server** page, including the server IP address, port number, shared key, and protocol. See the figure below.

RADIUS Server

Server IP: 200.200.0.95

Port: 1812

Shared Secret:

Confirm: Test

Protocol: PAP

☒ Enable RADIUS authentication

Save and Apply

Dynamic Routing

On the **Dynamic Routing** page, you can set the SANGFOR equipment to exchange or learn routing information from other network equipment through RIP for the purpose of updating routing information dynamically. See the figure below.

Dynamic Routing

☐ Enable Routing Information Protocol (RIP)

☐ Enable password based authentication Password:

IP Address: Port:

☒ Triggered periodic updates

Interval(sec):

☐ Log events

Save and Apply

Enable Routing Information Protocol: After this check box is selected, the SANGFOR VPN equipment advertises to the preset internal routing equipment the information about the peer network that establishes a VPN connection with the local end. This is to update the routing table on other equipment and add a route to the peer end, which directs to the SANGFOR VPN equipment. After the VPN connection is released, the routing equipment is notified to delete this route.

Enable password based authentication: authentication password for exchanging RIP information. Generally it does not need to be set.

IP Address and Port: IP address to which route updates are to be sent.

Triggered periodic updates: After this check box is selected, the equipment triggers route updating only when a system route change, and the **Interval** parameter is invalid.

Log events: If this check box is selected, the equipment records detailed RIP route update information.

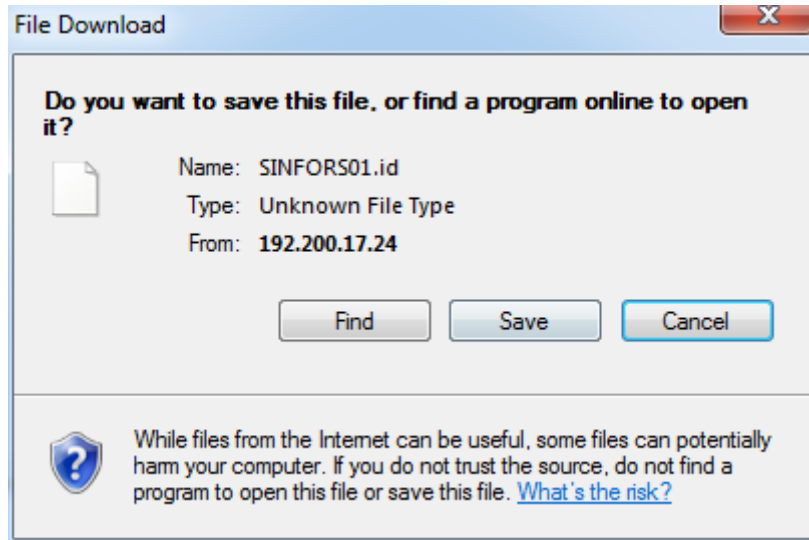
Certificate Generation

The hardware-based certificate authentication system is a patent of SANGFOR. The SANGFOR equipment adopts hardware-based certificate authentication to implement identity authentication between VPN nodes. A hardware feature is extracted for generating an encrypted authentication certificate. The certificate is unique and cannot be forged because the hardware feature is unique. This ensures that only the specified hardware equipment is authorized to access the network, avoiding security threats.

Click **Generate** and select a path for saving the hardware certificate on the local computer. See the figures below.

Certificate Generation

Generate



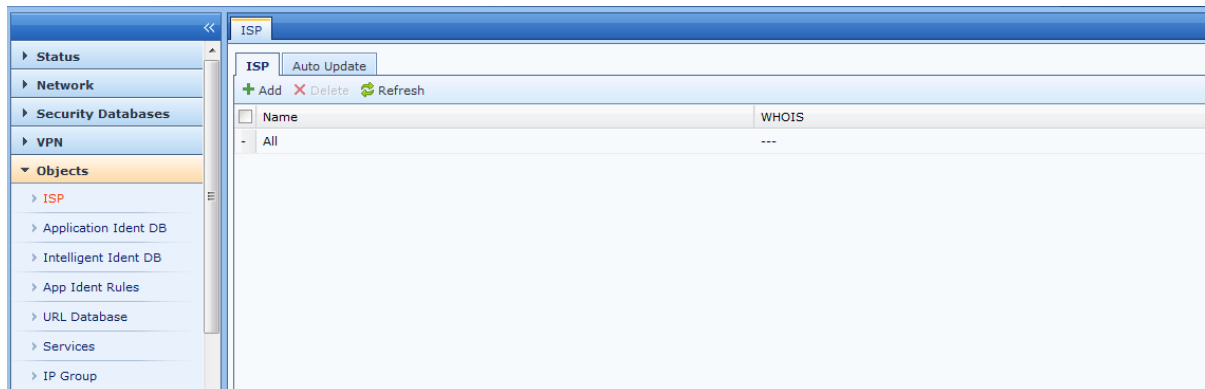
Send the generated certificate to the administrator at the headquarters. The administrator selects hardware authentication when creating a VPN account and binds the account with the hardware certificate.

Objects

Various objects defined in the **Objects** configuration module lay a foundation for the **Bandwidth Mgt**, **Firewall**, and **Access Control** configuration modules. Policy control and security control are exercised based on objects.

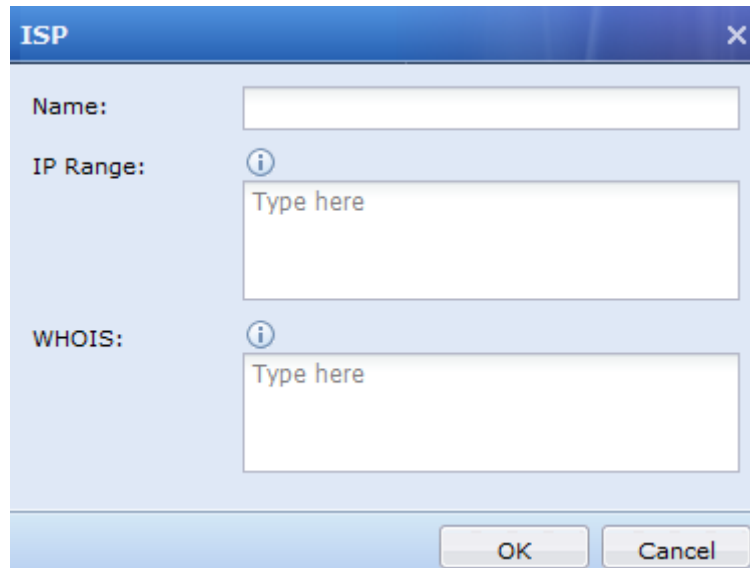
ISP

The **ISP** panel is used to set an IP address segment for the network operator, and the IP address segment is used to invoke multi-path load routing on the **Policy-Based Routing** tab page.



Click **Delete** to delete selected ISP information.

Click **Add** to add ISP information. See the figure below:



The image shows a dialog box titled "ISP" with a close button (X) in the top right corner. It contains three input fields: "Name:" with an empty text box; "IP Range:" with an information icon (i) and a text box containing "Type here"; and "WHOIS:" with an information icon (i) and a text box containing "Type here". At the bottom right, there are "OK" and "Cancel" buttons.

Name: ISP name.

IP Range: network IP address segment of the operator.

WHOIS: a WHOIS identifier corresponding to the ISP address segment. It is used to identify IP addresses of different operators.

Application Ident DB

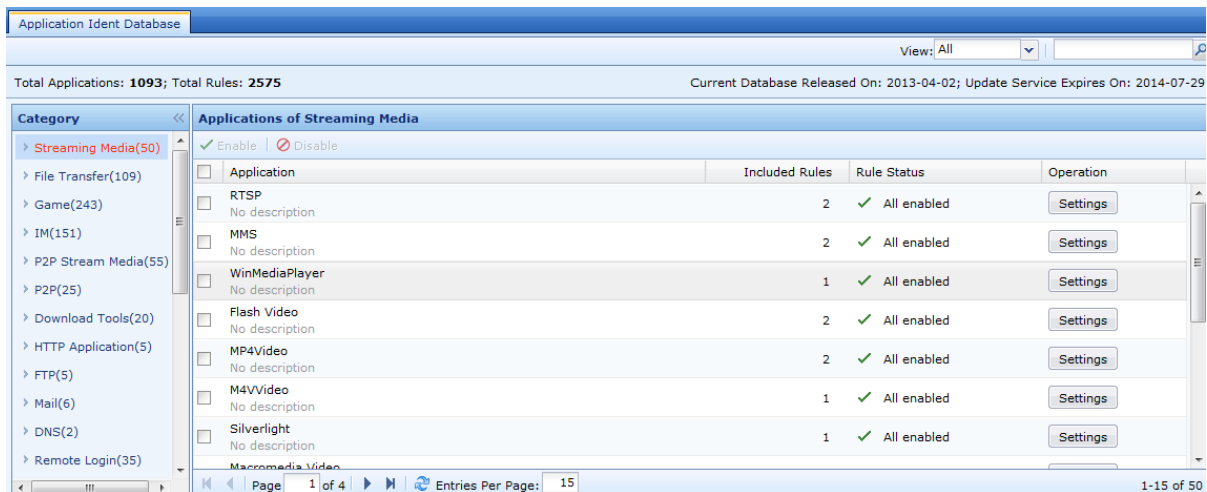
The application identification database is used to identify application types of network access data. It detects application types based on multiple conditions such as the characteristic value of a data packet, protocol, port, direction, data packet length, and data packet content, and can detect application types that cannot be distinguished by ports or protocols, for example, QQ and P2P.

The application identification database stores embedded rules and custom rules. Embedded rules cannot be modified and are periodically updated by the equipment. To update the embedded rules, a sequence number must be authorized, and network must be available for the equipment. Custom rules can be added, deleted, and modified. For details, see section 3.4.5.

To cite application identification rules and control related applications, choose **Access Control > Application Control Policy**.

Viewing Application Identification Rules

In the navigation area, choose **Objects > Application Ident DB**. The **Application Ident Database** page is displayed on the right.



Total Applications: 1093; Total Rules: 2575 displays the total number of applications and rules in the embedded rule identification database of the equipment.

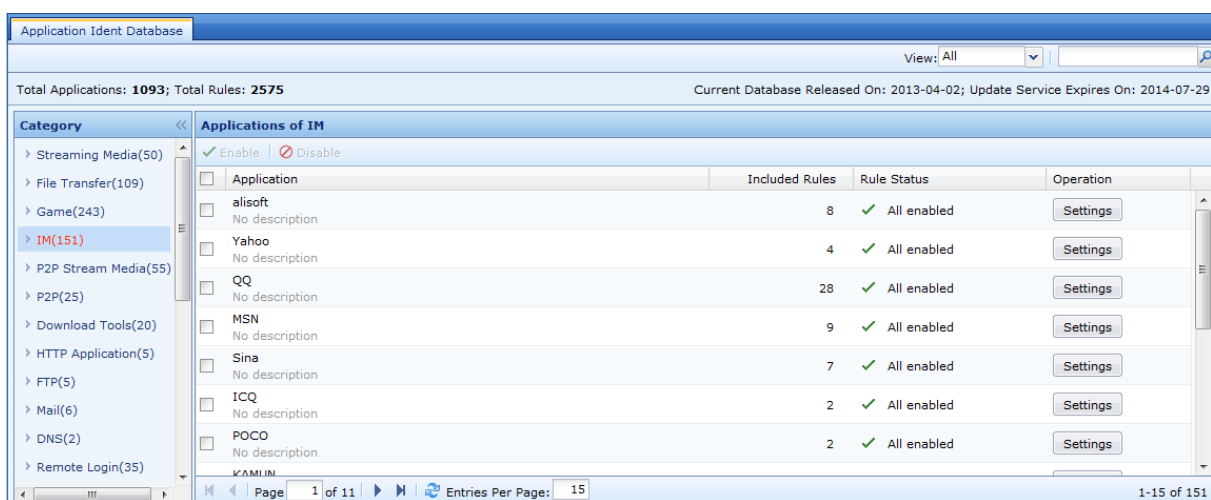
Current Database Released On displays the current version of the embedded rule identification database.

Update Service Expires On displays the upgrade expiry date of the embedded rule identification database.

Category displays the types of application identification rules, such as **IM** and **Game**.

Select an application type, and specific applications of the type are displayed on the right, for example, the QQ and MSN applications of the IM type.

Select the application type that you want to query from the **View** drop-down list box. If you select **All**, all rules that meet the search criteria are displayed. If you select **Enabled**, enabled rules that meet the search criteria are displayed. If you select **Disabled**, disabled rules that meet the search criteria are displayed. Type a keyword in the search box, for example, **QQ**, and press **Enter**. The figure below is displayed:



Enabling/Disabling Application Identification Rules

In the navigation area, choose **Objects > Application Ident DB**. The **Application Ident Database** page is displayed on the right. Query an application whose rules you want to set. For details, see section 3.4.2. For example, if you want to disable the rules for QQ, query QQ-related applications as follows:

Application Ident Database

View: All QQ

Total Applications: 1093; Total Rules: 2575

Current Database Released On: 2013-04-02; Update Service Expires On: 2014-07-29

Category	Applications of IM			
<div>File Transfer(4)</div> <div>Game(25)</div> <div>IM(7)</div> <div>P2P Stream Media(2)</div> <div>Remote Login(1)</div> <div>Soft-update(2)</div> <div>Stock-Quotation(1)</div> <div>Living services(3)</div>	<div><div>Enable</div><div>Disable</div></div>			
	Application	Included Rules	Rule Status	Operation
	<div><input type="checkbox"/></div> QQ No description	28	<div><div>✓</div>All enabled</div>	<div>Settings</div>
	<div><input type="checkbox"/></div> Web-QQ No description	7	<div><div>✓</div>All enabled</div>	<div>Settings</div>
	<div><input type="checkbox"/></div> QQ Voice Video No description	6	<div><div>✓</div>All enabled</div>	<div>Settings</div>
	<div><input type="checkbox"/></div> QQ-mobile No description	13	<div><div>✓</div>All enabled</div>	<div>Settings</div>
	<div><input type="checkbox"/></div> QQTalk No description	2	<div><div>✓</div>All enabled</div>	<div>Settings</div>
	<div><input type="checkbox"/></div> QQ drift bottles No description	2	<div><div>✓</div>All enabled</div>	<div>Settings</div>
	<div><input type="checkbox"/></div> Enterprise QQ No description	3	<div><div>✓</div>All enabled</div>	<div>Settings</div>

Page 1 of 1

Entries Per Page: 15

1-7 of 7

Select **QQ**, and click **Enable** or **Disable**. All rules for QQ are enabled or disabled.

If you want to enable or disable a certain rule for a specific application, for example, disable a certain rule for QQ, click **Settings**. The **QQ Identification Rule** dialog box is displayed and lists all QQ-related rules. Select a rule, click **Enable** or **Disable**. The selected rule is enabled or disabled.

QQ Identification Rule

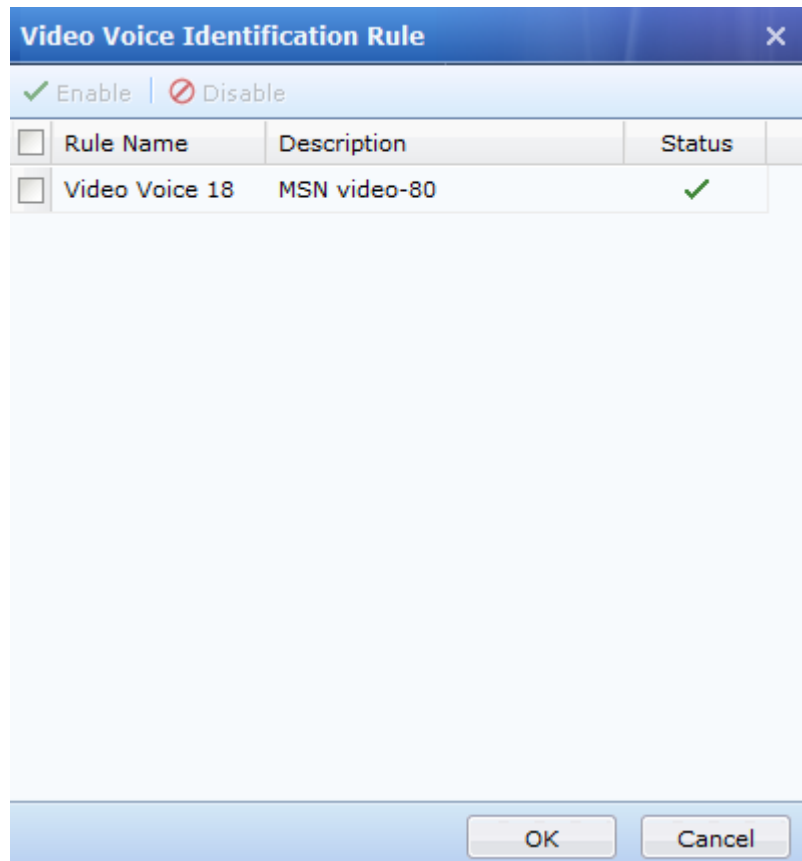
☒ Enable
 ☐ Disable

Rule Name	Status
<input type="checkbox"/> QQ[UDP]	✓
<input type="checkbox"/> QQ[TCP]	✓
<input type="checkbox"/> TM2008[udpsock]	✓
<input type="checkbox"/> QQ-P2P[U]	✓
<input type="checkbox"/> QQ[T]	✓
<input type="checkbox"/> QQ-TM[U]	✓
<input type="checkbox"/> QQ-P2P[T]	✓
<input type="checkbox"/> QQ-TM data	✓
<input type="checkbox"/> QQ-TM data[D]	✓
<input type="checkbox"/> QQ-TM data[U]	✓
<input type="checkbox"/> QQ-TM[UDP]	✓
<input type="checkbox"/> QQ-TM[TCP]	✓
<input type="checkbox"/> QQ-MSG[U]	✓
<input type="checkbox"/> QQ-MSG[T]	✓

OK

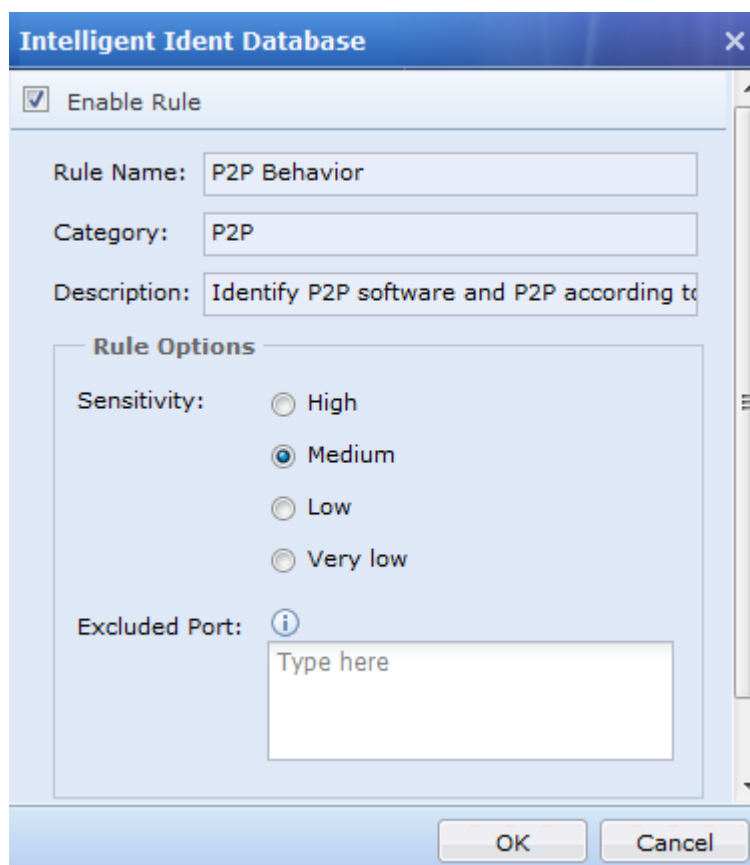
Cancel





Editing P2P Behavior Identification Rules

P2P behavior identification rules are supplements to the application identification rules and are used to identify P2P data that cannot be identified by the application identification database. P2P behavior rules can be edited. Click **P2P Behavior**. The **Intelligent Ident Database** dialog box is displayed.



Enable Rule: Select this check box to enable the rule.

Rule Name: name of the intelligent identification rule.

Category: application type of the rule.

Description: brief description of the rule.

The previous three items cannot be edited.

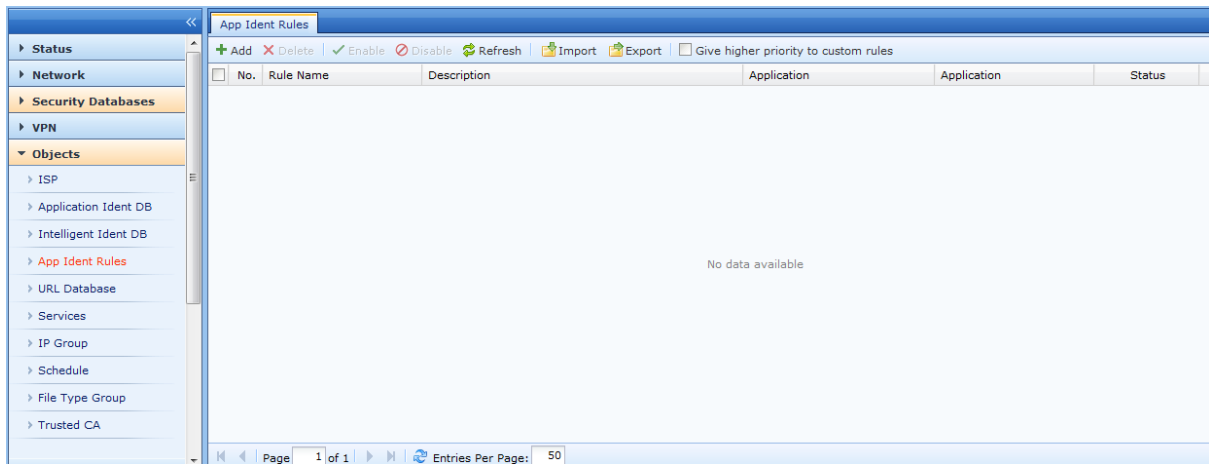
Sensitivity: sensitivity of the rule. It can be set to **High**, **Medium**, **Low**, or **Very Low** as required. Errors may occur during intelligent P2P identification. Therefore, set **Sensitivity** to adjust the identification criteria. Sensitivity decreases as the value is set from **High** to **Very Low**. Adjust the sensitivity based on specific data identification conditions. For example, if a large amount data needs to be identified, the data is connected to random high-end ports, and the destination IP addresses are unknown, the data may be unidentified P2P data. In this case, increase the sensitivity. If other types of data are mistaken as P2P data, the sensitivity may be too high. In this case, decrease the sensitivity.

Excluded Port: excluded ports. If destination ports of data are excluded ports, the equipment does not perform intelligent P2P identification on the data, which avoids identification errors.

App Ident Rules

The **App Ident Rules** panel is used to define application identification rules. You can define applications that are not contained in the embedded application identification database by setting the data direction, IP address, protocol, and port.

In the navigation area, choose **Objects > App Ident Rules**. The **App Ident Rules** page is displayed on the right.



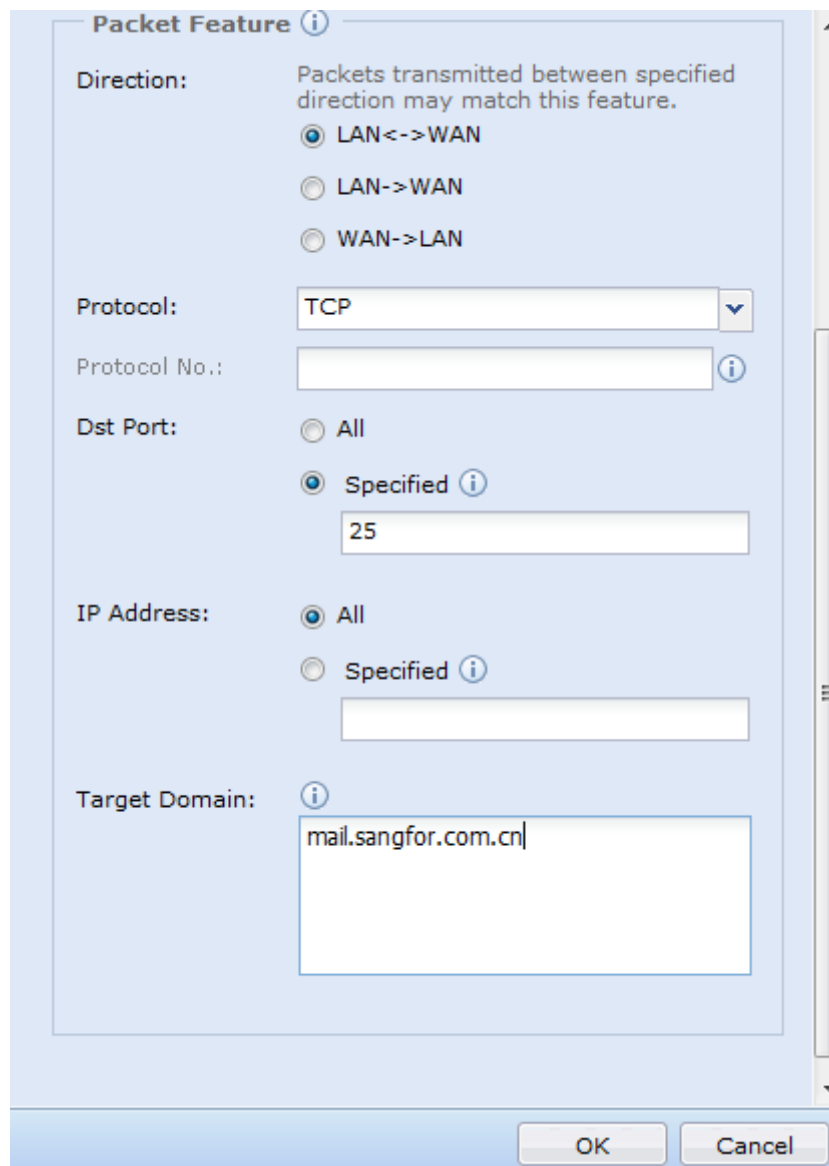
Adding Custom Application Rules

Click **Add** on the **App Ident Rules** page. The dialog box for adding custom application rules are displayed. Details are as follows:

Configuration example: Office email traffic needs to be controlled, but emails cannot be selected independently when a user selects an application type. In this case, an office email application can be defined.

Step 1: Enable rules and set **Basic Attributes**, including **Rule Name**, **Description**, **Category**, and **Application**. (You can select an existing category or define a new one.)

Step 2: Set Packet Feature.



Packet Feature ⓘ

Direction: Packets transmitted between specified direction may match this feature.

☒ LAN<->WAN

☐ LAN->WAN

☐ WAN->LAN

Protocol: TCP ▾

Protocol No.: ⓘ

Dst Port: ☐ All ☒ Specified ⓘ

25

IP Address: ☒ All ☐ Specified ⓘ

Target Domain: ⓘ

mail.sangfor.com.cn

OK Cancel

Direction: direction in which the data passes through the equipment. Only data in the direction will be identified.

Protocol: protocol type for the data. In this example, emails are sent over the TCP protocol.

Dst Port: destination port of the data. In this example, emails are sent over TCP25 ports.

IP Address: source IP address, destination IP address, or destination IP address identified by the proxy.

Target Domain: destination domain name accessed by the data. In this example, it is set to the domain name email address of the office, for example, **mail.sangfor.com.cn**.

Step 3: After the settings are completed, click **OK**.

App Ident Rules							
+ Add - Delete ✓ Enable ✗ Disable ↻ Refresh 📁 Import 📁 Export <input type="checkbox"/> Give higher priority to custom rules							
<input type="checkbox"/>	No.	Rule Name	Description	Application	Application	Status	Delete
<input type="checkbox"/>	1	Office Email	Office Email	Mail	Customize Email	✓	✗

Step 4: Set a priority for the custom rule. The embedded application identification database also stores email identification rules. If the embedded email rules have a higher priority, data may match the embedded email rules instead of the custom office email rule. Therefore, a priority must be set for the custom rule. Select **Give higher**

priority to custom rules on the **App Ident Rules** page.

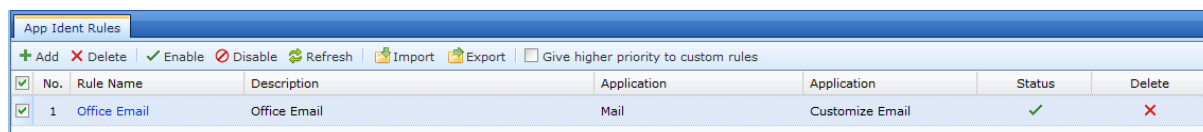
Step 5: Choose **Bandwidth Mgt > Bandwidth Channel**, and set a guaranteed channel for the application to ensure bandwidth for sending office emails. For details, see section 3.12.3.1.



You are advised to add identification information such as the destination port, IP address, and domain name when you set a custom rule. If the identification conditions are too general, they may conflict with the embedded application identification rules, causing identification errors and control and auditing failures.

Enabling/Disabling/Deleting Custom Application Rules

On the **App Ident Rules** page, select a custom rule, and click **Enable**, **Disable**, or **Delete**. The custom rule is enabled, disabled, or deleted.

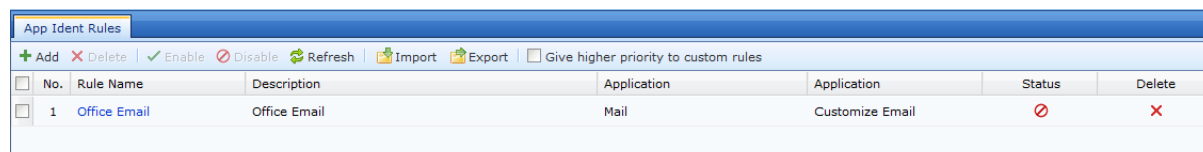


App Ident Rules							
+ Add - Delete ✓ Enable ✗ Disable ↻ Refresh 📁 Import 📁 Export <input type="checkbox"/> Give higher priority to custom rules							
<input checked="" type="checkbox"/>	No.	Rule Name	Description	Application	Application	Status	Delete
<input checked="" type="checkbox"/>	1	Office Email	Office Email	Mail	Customize Email	✓	✗

Importing/Exporting Custom Application Rules

Click **Import** to import a custom application rule.

Click **Export** to export a custom application rule.



App Ident Rules							
+ Add - Delete ✓ Enable ✗ Disable ↻ Refresh 📁 Import 📁 Export <input type="checkbox"/> Give higher priority to custom rules							
<input type="checkbox"/>	No.	Rule Name	Description	Application	Application	Status	Delete
<input type="checkbox"/>	1	Office Email	Office Email	Mail	Customize Email	✗	✗

URL Database

The URL database defines different URL types based on the content on web pages, which helps the equipment identify various websites and exercise access permission control and traffic control on various websites. The **URL Database** page displays embedded URL groups and custom URL groups. Embedded URL groups are periodically updated on the server by SANGFOR. The equipment updates the embedded URL groups by accessing the server based on authorization. When the embedded URL groups do not meet your requirements, you can set custom URL groups based on known URLs.

URL Database

The **URL Database** page displays embedded URL databases and custom URL databases. Embedded URL

databases are periodically updated by the equipment. To update the embedded databases, a sequence number must be authorized, and network must be available for the equipment. Custom URL databases can be added, deleted, and modified. For details, see section 3.4.7.

In the navigation area, choose **Objects > URL Database**. The **URL Database** page is displayed on the right. Click on the **URL Database** page. The version and upgrade expiry date of the embedded URL database are displayed in the upper part of the page.

URL Database			
+ Add X Delete Refresh Q URL Category Lookup Database Version: 2013-04-28 Update Service Expires On: 2014-07-29			
URL Category	Description	Type	Delete
Job-hunting & Employment	Websites containing job-hunting and recruitment information.	Internal	X
Adult Content	Websites that contain information and comments on adult products, sex education, nude, body art, adults' ent...	Internal	X
Online Shopping	Websites providing online shopping and online shopping services.	Internal	X
News Portal	Websites that contain latest news and comments on current affairs, including the websites created by media s...	Internal	X
IT Related	Websites providing information of IT industry, IT figures, program designing and network, and the forums for...	Internal	X
Education	Websites of various culture and education institutions, and websites marketing or providing references for ed...	Internal	X
Religion	Websites of religion administrative departments of the nation, and websites of various religion organizations a...	Internal	X
Nonprofit Organization	Websites created by the non-profit social organizations, such as charity institution, volunteer organization, tra...	Internal	X
Science & Technology	Websites that research the existence of object things and related regularity and that provide science and tech...	Internal	X
Web Application			
Microblog	Informal mini blog that is similar to traditional blog and publishes instant messages.	Internal	X
Web Mailbox	Websites that provide email-related services.	Internal	X
Search Engine	Websites providing search service, webpage list and index service.	Internal	X
Forum	Various websites that provide visitors with forum for leaving message, BBS, etc., excluding the websites prov...	Internal	X
Online Chat	Web version of instant messaging (IM) tools, and websites that offers chat room to send and receive instant ...	Internal	X
Network Storage	Websites that store files on the Internet server for backup or sharing.	Internal	X
Software Download	Websites providing various software download.	Internal	X

3.5.5.1.1 Querying a URL Category

In the navigation area, choose **Objects > URL Database**. The **URL Database** page is displayed on the right. Click [Q URL Category Lookup](#). The **URL Category Lookup** dialog box is displayed. Set **Domain Name** and click **Go**.

The corresponding URL category is displayed.

URL Category Lookup

Domain Name:

Result: The URL category you are searching for is
[Search Engine]



Fuzzy search is not supported.

3.5.5.1.2 Adding a URL Category

You can add a custom URL category. On the **URL Database** page, click **Add**. The **Add URL Category** dialog box is displayed.

Name: name of the URL category.

Description: description of the URL category.

URL: URL category to be set. A URL category may contain multiple URLs, which support wildcard-based matching.

URL Keyword: keyword for automatically matching a URL category. A domain name containing the keyword is identified as the URL category. The matching priority of domain name keywords is lower than that of embedded URL databases and custom URL databases.



The asterisk (*) is a wildcard character. For example, if you want to set a URL for Sina web pages, including news.sina.com.cn, sports.sina.com.cn, and ent.sina.com.cn, type *.sina.com.cn in the URL text box. Note that the asterisk (*) indicates only matching of top-level domain names, and it must be placed in front of the URL for the URL to take effect.

3.5.5.1.3 Deleting a URL Category

You can delete a custom URL category. Embedded URL categories on the equipment cannot be deleted. On the **URL Database** page, select a custom URL category, and click **Delete**. The selected URL category is deleted.

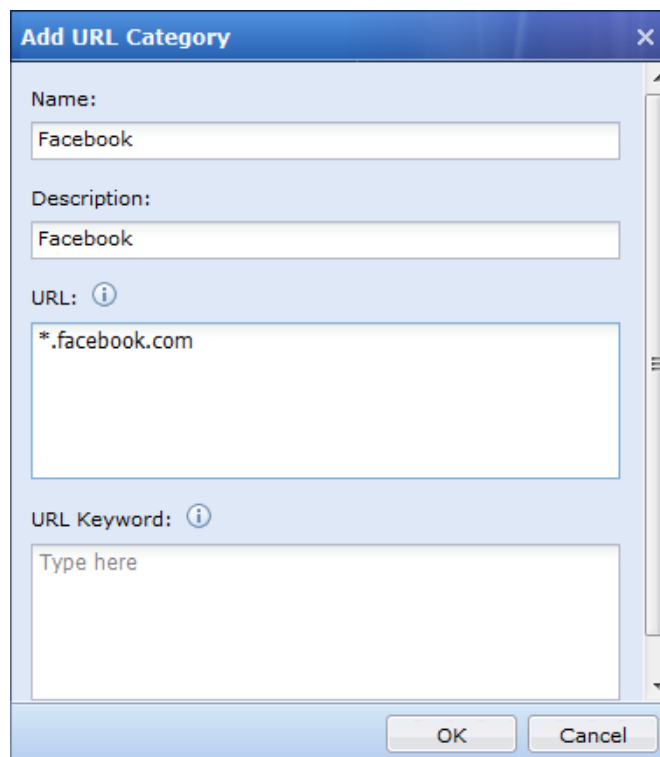
3.5.5.1.4 Modifying a URL Category

You can modify a custom URL category or an embedded URL category.

When you edit a custom URL category, you can edit **Description**, **URL**, and **URL Keyword**.

When you edit an embedded URL category, you cannot edit **Name** or **Description** or edit an existing URL in the embedded URL databases. You can only add URLs and keywords in the **URL** and **URL Keyword** text boxes as supplements to the embedded URL databases.

Click the name of the URL category that you want to modify. The **Add URL Category** dialog box is displayed.

The image shows a dialog box titled "Add URL Category" with a close button (X) in the top right corner. The dialog box contains four input fields: "Name:" with the text "Facebook", "Description:" with the text "Facebook", "URL:" with the text "*.facebook.com" and an information icon (i) to its left, and "URL Keyword:" with the text "Type here" and an information icon (i) to its left. At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

Services

Services are a group of specific protocols and ports. They generally indicate certain network applications and can be invoked by the **Application Control Policy** panel of the **Access Control** configuration module to allow or reject certain network services.

Predefined Services

Common network services are embedded on the **Predefined Service** tab page. See the figure below:

Services	
Predefined Service	Custom Services
Name	Protocol
any	TCP:0-65535; UDP:0-65535; ICMP:type 0-255, code 0-255;
bgp	TCP:179;
cluster	UDP:3343;
dns-t	TCP:53;
dns-u	UDP:53;
ftp	TCP:21;
h.225	TCP:1720;
h.225ras	UDP:1719;
http	TCP:80;
https	TCP:443;
irc	TCP:194;
l2tp	UDP:1701;
ldap	TCP:389;
ms-sql-m	TCP:1434;
ms-sql-r	UDP:1434;
ms-sql-s	TCP:1433;
mysql	TCP:3306;
netbios-ns	UDP:137;

The **Predefined Service** tab page displays default ports of common protocols, which cannot be edited or modified. If the predefined services do not meet your requirements, set **Custom Services**.

Custom Services

On the **Custom Services** tab page, click **Add**. The **Add Custom Service** dialog box is displayed.

Add Custom Service

Name:

Description:

Protocol:

TCP

UDP

ICMP

Other

Type here

OK

Cancel

Name: service name.

Description: service description.

Protocol: protocol type and port number of the service. Click **TCP**, **UDP**, **ICMP**, and **Other** in sequence, and add the corresponding port in the text box.

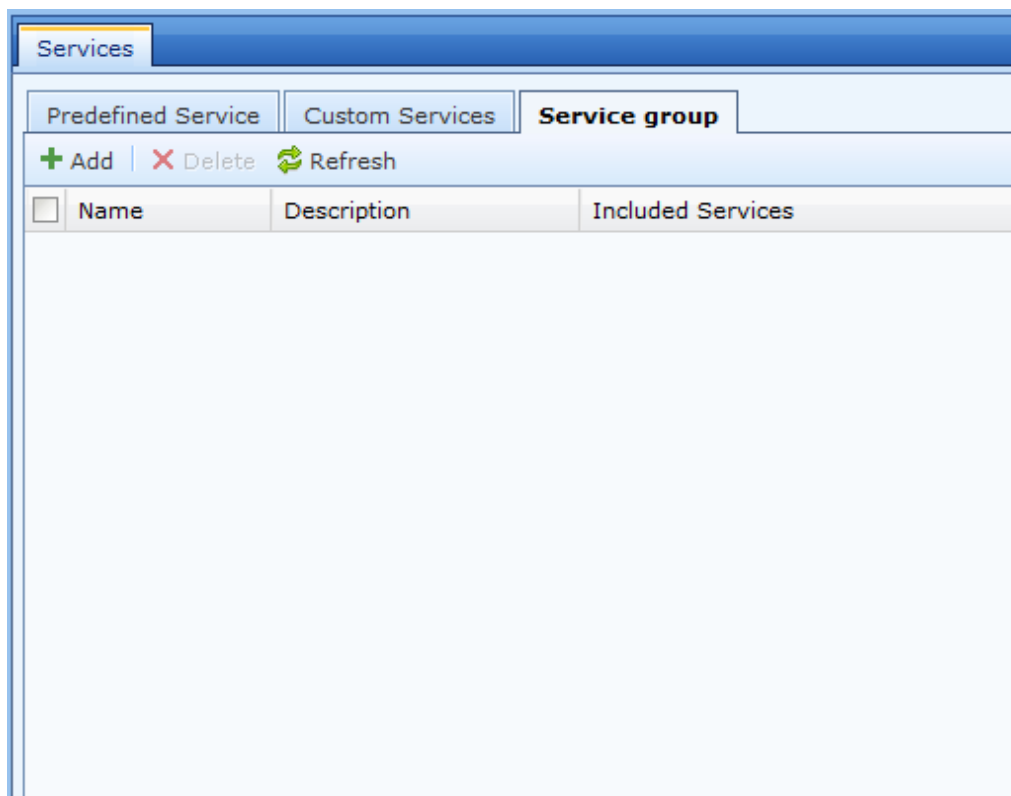
Click **OK**. Network services are set properly.



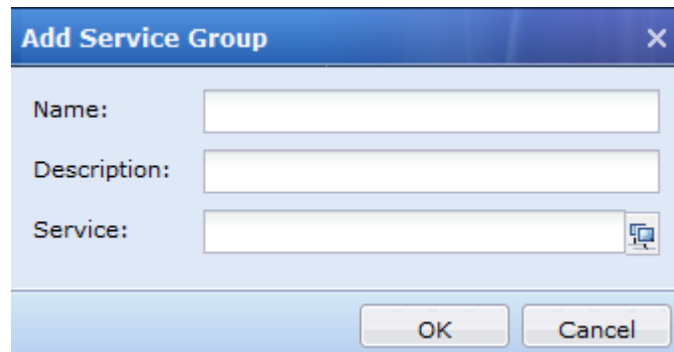
- You can type a protocol number in the **Other** text box. 0 indicates all protocols. The protocol number is an integer ranging from 0 to 255.
- In the **TCP** or **UDP** text box, type one port or one port range in a row. In the **ICMP** text box, set ports in the type:*a*,code:*b* format. *a* and *b* are integers ranging from 0 to 255. Multiple rows can be input.

Service Groups

On the **Service group** tab page, multiple services can be combined into one service group. When multiple services need to be referenced, you can directly reference the corresponding service group. See the figure below:



Click **Add**. The **Add Service Group** dialog box is displayed, as shown in the figure below:



The 'Add Service Group' dialog box has a blue title bar with the text 'Add Service Group' and a close button (X). It contains three input fields: 'Name:', 'Description:', and 'Service:'. The 'Service:' field has a small icon to its right. At the bottom, there are 'OK' and 'Cancel' buttons.

Name: service group name.

Description: service group description.

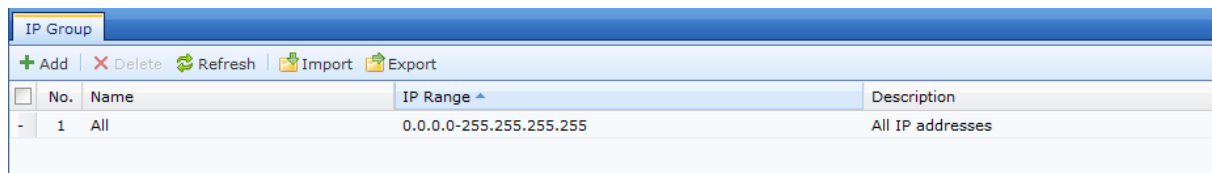
Service: services contained in the service group. Click  to select services. You can select multiple services from the predefined services and custom services.

IP Group

The **IP Group** panel is used to define an IP address group that contains certain IP addresses. The IP address group may contain an IP address segment on the LAN, an IP address segment on the Internet, or all IP addresses. Both IPv4 and IPv6 IP address are supported.

The settings on the **IP Group** panel can be referenced by the **NAT** panel of the **Firewall** configuration module, **Application Control Policy** panel of the **Access Control** configuration module, and **Bandwidth Channel** panel of the **Bandwidth Mgt** configuration module.

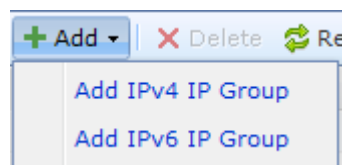
In the navigation area, choose **Objects > IP Group**. The **IP Group** page is displayed on the right.



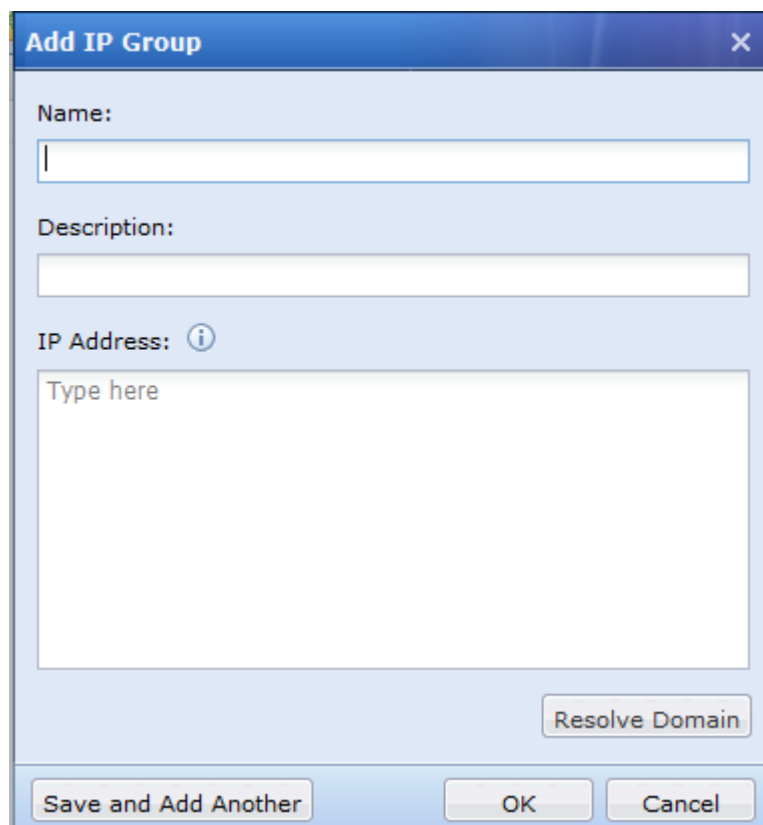
The screenshot shows the 'IP Group' panel with a toolbar containing '+ Add', 'X Delete', 'Refresh', 'Import', and 'Export'. Below the toolbar is a table with the following data:

No.	Name	IP Range	Description
1	All	0.0.0.0-255.255.255.255	All IP addresses

On the **IP Group** page, click **Add** to select IPv4 or IPv6 group.



Click on **Add IPv4 IP Group** or **Add IPv6 IP Group**. The **Add IP Group** dialog box is displayed.



The 'Add IP Group' dialog box contains the following fields and buttons:

- Name:** A text input field for the IP group name.
- Description:** A text input field for the IP group description.
- IP Address:** A large text area with a placeholder 'Type here' for entering IP addresses or ranges. An information icon (i) is next to the label.
- Buttons:** 'Resolve Domain', 'Save and Add Another', 'OK', and 'Cancel' are located at the bottom.

Name: IP group name.

Description: IP group description.

IP Address: Type one IP address or IP address range in a row. The IP address range is in the *start IP address–end IP address* format, for example, **192.168.0.1–192.168.0.100** or **2001::1001-2001::f000**.

Resolve Domain: indicates automatically resolving IP addresses corresponding to certain domain names. This function can automatically add resolved IP addresses to the IP address list.



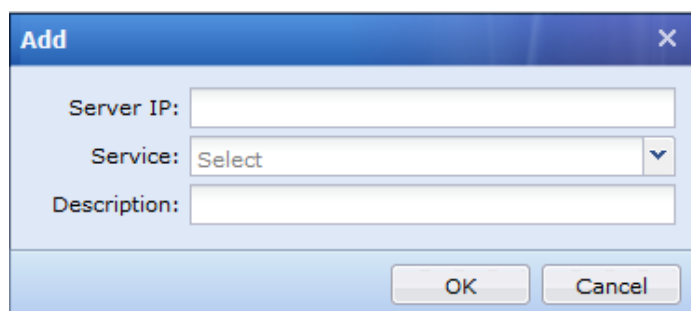
The Resolve Domain function is implemented by the equipment. Therefore, the equipment must have access to network and is configured with available DNS addresses for resolving domain names.

LAN Server

The LAN Server panel is used to display manual added servers or auto identified servers by NGAF.

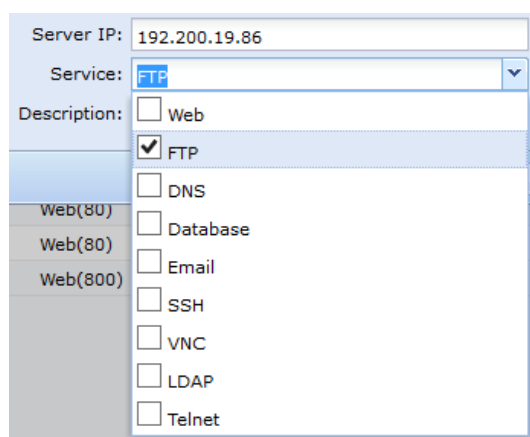
Navigation																																																											
<ul style="list-style-type: none"> Status Network Security Databases VPN Objects <ul style="list-style-type: none"> ISP Application Ident DB Intelligent Ident DB App Ident Rules URL Database Services IP Group LAN Servers 	<div>LAN Servers</div> <div> + Add × Delete ↻ Refresh </div> <table> <thead> <tr> <th>No.</th><th>Server IP</th><th>Service & Port</th><th>Description</th><th>Operation</th></tr> </thead> <tbody> <tr> <td colspan="5">Custom Servers</td></tr> <tr> <td>1</td><td>192.200.19.200</td><td>Web(808,80,8080,8081); FTP(21); Database(1433); Email(808)</td><td>TSC</td><td>Delete</td></tr> <tr> <td colspan="5">Auto Identified Servers</td></tr> <tr> <td>1</td><td>192.200.19.201</td><td>Web(80)</td><td>-</td><td>Excluded</td></tr> <tr> <td>2</td><td>192.200.19.220</td><td>LDAP(389)</td><td>-</td><td>Excluded</td></tr> <tr> <td>3</td><td>192.200.19.227</td><td>Web(85)</td><td>-</td><td>Excluded</td></tr> <tr> <td>4</td><td>192.200.19.228</td><td>Web(80)</td><td>-</td><td>Excluded</td></tr> <tr> <td>5</td><td>192.200.19.229</td><td>Web(80)</td><td>-</td><td>Excluded</td></tr> <tr> <td>6</td><td>192.200.19.231</td><td>Web(80)</td><td>-</td><td>Excluded</td></tr> <tr> <td>7</td><td>192.200.19.232</td><td>Web(800)</td><td>-</td><td>Excluded</td></tr> </tbody> </table>				No.	Server IP	Service & Port	Description	Operation	Custom Servers					1	192.200.19.200	Web(808,80,8080,8081); FTP(21); Database(1433); Email(808)	TSC	Delete	Auto Identified Servers					1	192.200.19.201	Web(80)	-	Excluded	2	192.200.19.220	LDAP(389)	-	Excluded	3	192.200.19.227	Web(85)	-	Excluded	4	192.200.19.228	Web(80)	-	Excluded	5	192.200.19.229	Web(80)	-	Excluded	6	192.200.19.231	Web(80)	-	Excluded	7	192.200.19.232	Web(800)	-	Excluded
No.	Server IP	Service & Port	Description	Operation																																																							
Custom Servers																																																											
1	192.200.19.200	Web(808,80,8080,8081); FTP(21); Database(1433); Email(808)	TSC	Delete																																																							
Auto Identified Servers																																																											
1	192.200.19.201	Web(80)	-	Excluded																																																							
2	192.200.19.220	LDAP(389)	-	Excluded																																																							
3	192.200.19.227	Web(85)	-	Excluded																																																							
4	192.200.19.228	Web(80)	-	Excluded																																																							
5	192.200.19.229	Web(80)	-	Excluded																																																							
6	192.200.19.231	Web(80)	-	Excluded																																																							
7	192.200.19.232	Web(800)	-	Excluded																																																							

Click **Add** to add the new LAN Servers. See the figure below.



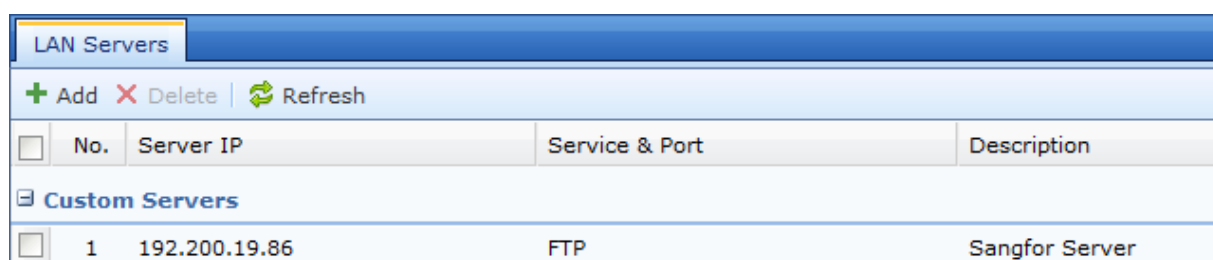
The 'Add' dialog box is a small window with a blue header bar containing the title 'Add' and a close button. It contains three input fields: 'Server IP' with a text box, 'Service' with a dropdown menu showing 'Select', and 'Description' with a text box. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

In the drop down list of **Service**, there are many types of services to choose.
Example, if it is a FTP Server, select **FTP** service.



This image shows the 'Service' dropdown menu expanded. The 'Server IP' field is filled with '192.200.19.86'. The 'Service' dropdown is set to 'FTP'. The 'Description' field has a list of checkboxes: 'Web', 'FTP' (checked), 'DNS', 'Database', 'Email', 'SSH', 'VNC', 'LDAP', and 'Telnet'. On the left side of the dropdown, there are labels for 'Web(80)', 'Web(80)', and 'Web(800)'.

Click **OK** to confirm the new LAN Server. The result will display at the **Customer Servers**.
See the figure below.



The 'LAN Servers' window shows a table with columns: 'No.', 'Server IP', 'Service & Port', and 'Description'. There is a '+ Add' button, a 'X Delete' button, and a 'Refresh' button. Below the table, there is a section for 'Custom Servers'.

No.	Server IP	Service & Port	Description
1	192.200.19.86	FTP	Sangfor Server

Schedule

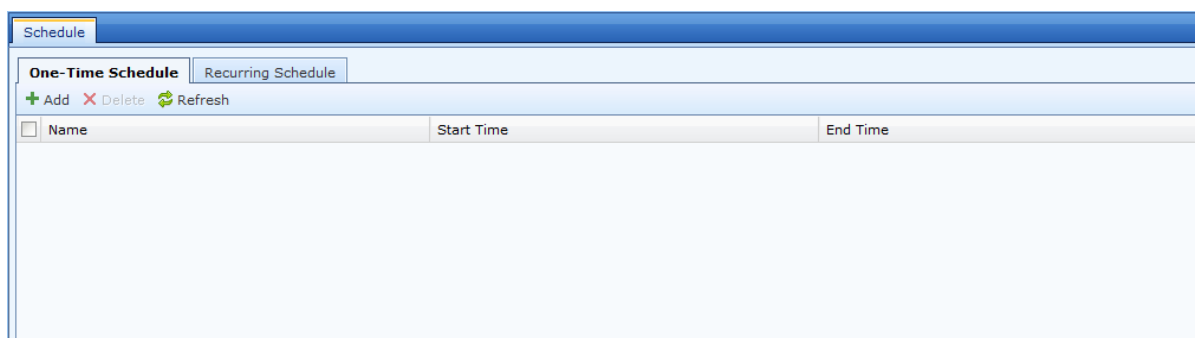
The **Schedule** panel is used to define common time segments, which can be selected on the **Application Control Policy** panel of the **Access Control** configuration module or the **Bandwidth Channel** of the **Bandwidth Mgt** configuration module, for setting the effective time or expiry time of the rules.

The one-time schedule and recurring schedule are available.

One-Time Schedule

The one-time schedule specifies the start date and time of a schedule, and the equipment executes the schedule within the specified time segment only once. The one-time schedule is usually applied to special dates. For example, you can specify an application control policy by using the schedule to prohibit games during the National Holiday. After the National Holiday elapses, the equipment automatically enables the game application, without manual intervention.

In the navigation area, choose **Objects > Schedule > One-Time Schedule**. The **One-Time Schedule** tab page is displayed.



On the **One-Time Schedule** tab page, click **Add**. The **Add One-Time Schedule** dialog box is displayed.

Name: schedule name.

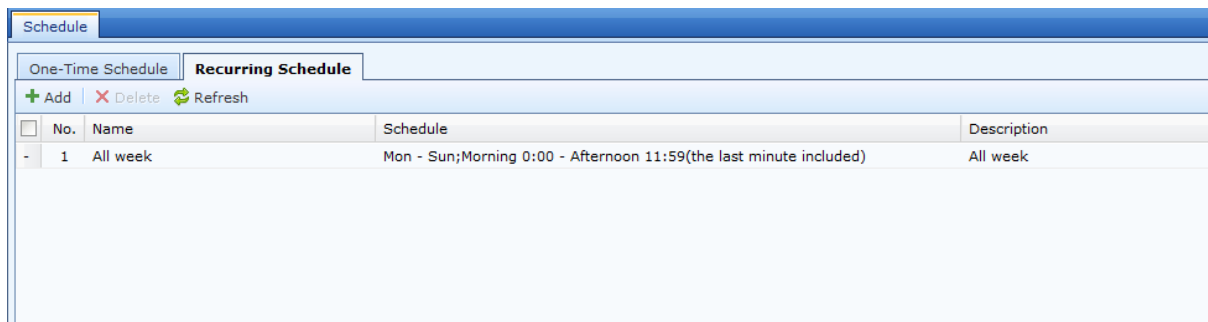
Start Time: start date and time of the schedule.

End Time: end date and time of the schedule.

Recurring Schedule

The recurring schedule specifies a certain time segment from Monday to Sunday, and the equipment cyclically executes the schedule within the specified time segment.

In the navigation area, choose **Objects > Schedule > Recurring Schedule**. The **Recurring Schedule** tab page is displayed.



On the **Recurring Schedule** tab page, click **Add**. The **Add Recurring Schedule** dialog box is displayed.

Days Of Week	Time Segment	Edit	Delete
No data available			

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon																								
Tue																								
Wed																								
Thu																								
Fri																								
Sat																								
Sun																								

Name: schedule name.

Description: schedule description.

Add Time Segment: Click **Add Time Segment** to set a specific time period and time range. See the figure below:

If you want to set several discontinuous time segments, add multiple time segments.

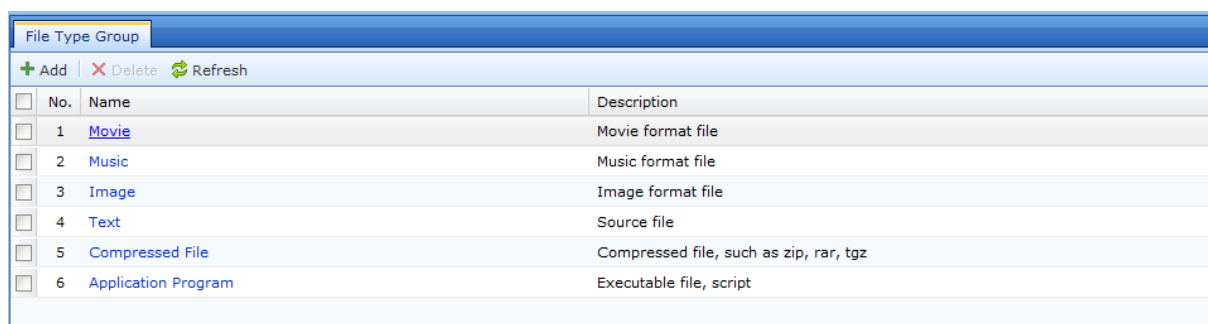
Delete: deletes time segments. Select a time segment that you want to delete, and click **Delete**. The selected time segment is deleted.

Schedule Preview: displays time segments. The horizontal axis indicates time points, and the vertical axis indicates a date range.

File Type Group

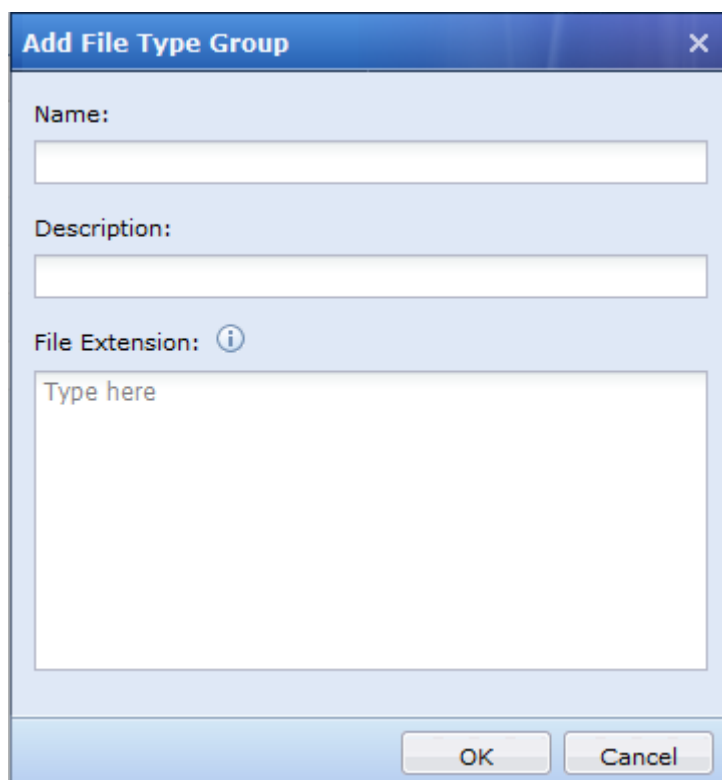
The **File Type Group** panel is used to define required file types, which can be applied to the **File Filter** tab page of the **Web Filter** panel of the **Access Control** configuration module for limiting upload and download of HTTP and FTP files, and can also be applied to the **Bandwidth Channel** tab page of the **Bandwidth Channel** panel of the **Bandwidth Mgt** configuration module for setting bandwidth control on file upload and download.

In the navigation area, choose **Objects > File Type Group**. The **File Type Group** page is displayed on the right.



<input type="checkbox"/>	No.	Name	Description
<input type="checkbox"/>	1	Movie	Movie format file
<input type="checkbox"/>	2	Music	Music format file
<input type="checkbox"/>	3	Image	Image format file
<input type="checkbox"/>	4	Text	Source file
<input type="checkbox"/>	5	Compressed File	Compressed file, such as zip, rar, tgz
<input type="checkbox"/>	6	Application Program	Executable file, script

On the **File Type Group** page, click **Add**. The **Add File Type Group** dialog box is displayed, as shown in the figure below:



Add File Type Group

Name:

Description:

File Extension: ⓘ

OK Cancel

Name: name of the file type group.

Description: description of the file type group.

File Extension: file name extension. Type various file name extensions, such as *.mp3 and mp3.



The equipment is configured with most file types by default, including movies, music, pictures, texts, compressed files, and application programs. If the file types do not meet your requirements, manually add file types.

Trusted CA

You can import certificates into or delete certificates from the certificate database.

In the navigation area, choose **Objects > Trusted CA**. The **Trusted CA** page is displayed on the right.

Trusted CA			
+ Upload Trusted Root CA X Delete Refresh			
<input type="checkbox"/>	No.	CA	
			<div>Valid FromTo</div>
<input type="checkbox"/>	1	UTN-USERFirst-Object	<div>Jul 9 18:31:20 1999 GMTJul 9 18:40:36 2019 GMT</div>
<input type="checkbox"/>	2	DST-Entrust GTI CA	<div>Dec 9 00:02:24 1998 GMTDec 9 00:32:24 2018 GMT</div>
<input type="checkbox"/>	3	Swisskey Root CA	<div>Apr 15 10:38:00 1999 GMTDec 31 23:59:00 2015 GMT</div>
<input type="checkbox"/>	4	AddTrust External CA Root	<div>May 30 10:48:38 2000 GMTMay 30 10:48:38 2020 GMT</div>
<input type="checkbox"/>	5	C&W HKT SecureNet CA Class A	<div>Jun 30 00:00:00 1999Oct 15 23:59:00 2009</div>
<input type="checkbox"/>	6	Equifax Secure eBusiness CA-2	<div>Jun 23 12:14:45 1999 GMTJun 23 12:14:45 2019 GMT</div>
<input type="checkbox"/>	7	First Data Digital Certificates Inc. Certification Authority	<div>Jul 3 18:47:34 1999 GMTJul 3 19:17:34 2019 GMT</div>
<input type="checkbox"/>	8	Class 3 Public Primary Certification Authority	<div>Jan 29 00:00:00 1996 GMTAug 1 23:59:59 2028 GMT</div>
<input type="checkbox"/>	9	Thawte Premium Server CA	<div>Aug 1 00:00:00 1996 GMTDec 31 23:59:59 2020 GMT</div>
<input type="checkbox"/>	10	IPS SERVIDORES	<div>Jan 1 23:21:07 1998 GMTDec 29 23:21:07 2009 GMT</div>
<input type="checkbox"/>	11	SecureSign RootCA1	<div>Sep 15 15:00:01 1999 GMTSep 15 14:59:59 2020 GMT</div>
<input type="checkbox"/>	12	DSTCA E2	<div>Dec 9 19:17:26 1998 GMTDec 9 19:47:26 2018 GMT</div>
<input type="checkbox"/>	13	FESTE, Public Notary Certs	<div>May 13 19:21:28 1999 GMTJan 1 19:21:28 2020 GMT</div>
<input type="checkbox"/>	14	SecureNet CA SGC Root	<div>Aug 20 00:43:29 1999 GMTOct 16 07:00:00 2009 GMT</div>
<input type="checkbox"/>	15	VeriSign Commercial Software Publishers CA	<div>Apr 9 09:35:59 1996 GMTDec 31 09:35:58 1999 GMT</div>

On the **Trusted CA** page, click **Upload Trusted Root CA**, and select and import a certificate. Only local .crt or .cer certificates can be imported.

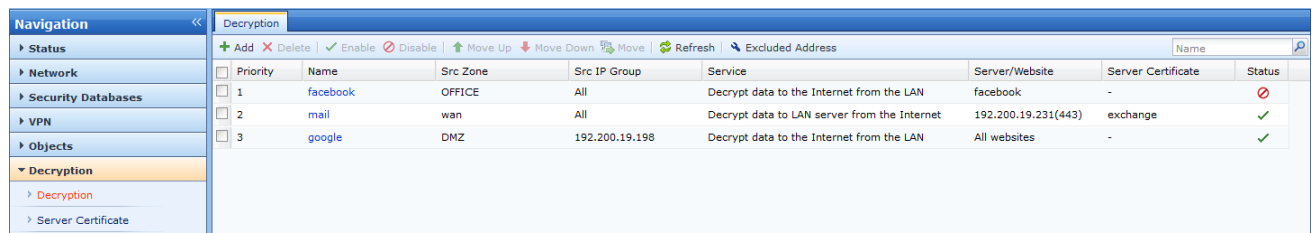
Certificates are distinguished based on their MD5 values. Certificates with different MD5 values are identified as different certificates. The same certificate cannot be imported repeatedly.



The name of the certificate theme is generally the CN name of the certificate theme in the Internet Explorer. If the certificate theme does not have a CN name, the name of the last field of the certificate theme is used. (The sequence of the fields of the certificate theme may be different from that in the Internet Explorer.)

Decryption

The **Decryption** configuration module is used to decrypt data from Internet to LAN and from LAN to Internet.



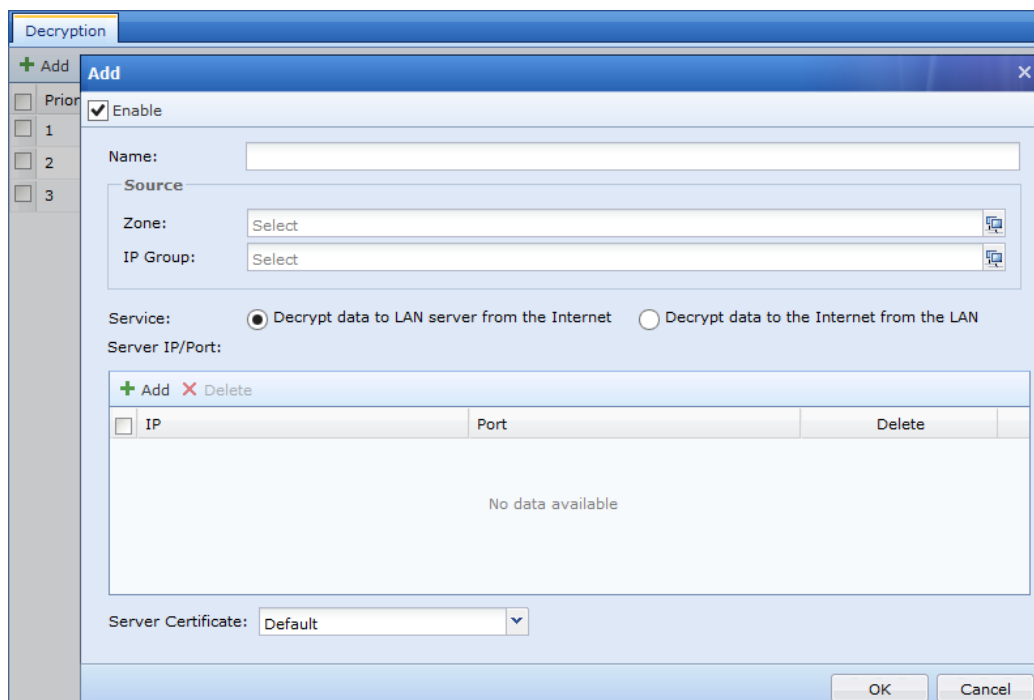
Priority	Name	Src Zone	Src IP Group	Service	Server/Website	Server Certificate	Status
1	facebook	OFFICE	All	Decrypt data to the Internet from the LAN	facebook	-	✗
2	mail	wan	All	Decrypt data to LAN server from the Internet	192.200.19.231(443)	exchange	✓
3	google	DMZ	192.200.19.198	Decrypt data to the Internet from the LAN	All websites	-	✓

Decryption

This function used to decrypt SSL data from internet to LAN. After decryption, NGAF WAF can detect attack.

This function used to decrypt SSL data from LAN to internet. After decryption, NGAF can audit and control HTTPS action. Such as only allow users to view Facebook, but cannot post status.

Click **Add** to insert new decryption configuration.



Add

☒ Enable

Name:

Source

Zone:

IP Group:

Service: ☒ Decrypt data to LAN server from the Internet ☐ Decrypt data to the Internet from the LAN

Server IP/Port:

IP	Port	Delete
No data available		

Server Certificate:

OK Cancel

Name: The name of new decryption configuration

Source Zone: Source zone that wants to be decrypted

IP Group: IP Group that wants to be decrypted

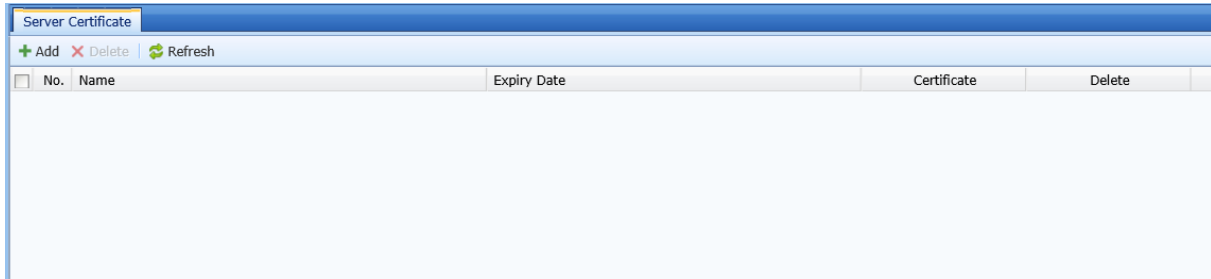
Service: Decrypt data to LAN server from the Internet or Internet from the LAN

Server IP/Port: Add the Server IP and using port number

Server Certificate:

Server Certificate

Server Certificate is an object used in the SSL Policy Configuration, there are 3 methods to add a server certificate in this sections: Import Certificate, Self-signed Certificate and Import Public/Private Key. Navigate to **Objects > Server Certificate** and the page is shown as figure below:



Import Certificate

Click on **Add** and select **Import Certificate** the page below is shown:

A dialog box titled "Import Certificate" with a close button (X) in the top right corner. It contains three input fields: "Name:" followed by a text box; "Certificate:" followed by a text box containing "*.pfx, *.p12" and a "Browse..." button; and "Password:" followed by a text box. At the bottom right are "OK" and "Cancel" buttons.

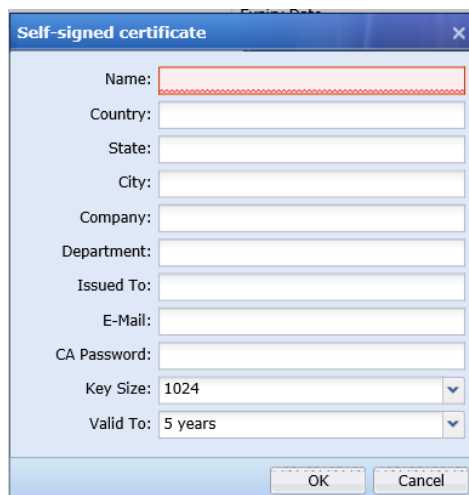
Name: Name for the Certificate object.

Certificate: Click on **Browse** to select certificate which default format .pfx and . p12 for this object.

Password: Insert the password of certificate.

Self-signed Certificate

Click on **Add** and select **Self-signed Certificate** the page below is shown:

A dialog box titled "Self-signed certificate" with a close button (X) in the top right corner. It contains several text input fields: "Name:", "Country:", "State:", "City:", "Company:", "Department:", "Issued To:", "E-Mail:", and "CA Password:". Below these are two dropdown menus: "Key Size:" set to "1024" and "Valid To:" set to "5 years". At the bottom are "OK" and "Cancel" buttons.

Configure the required fields. In this scenario, **Name, Country, State, City, Company, Department, Email address, the certificate is issued to, CA Password, Key Size, and Valid period.**

Click **OK** to complete the process.

Import Public/Private Key

Click on **Add** and select **Import Public/Private Key** the page below is shown:

A dialog box titled "Import Public/Private Key" with a close button (X) in the top right corner. It contains a "Name:" text input field. Below it are two sections: "Public Key:" and "Private Key:". Each section has radio buttons for "File" (selected) and "Text". Under "Public Key:", there is a "File:" text input field with the pattern "*.PEM, *.DER" and a "Browse..." button. Under "Private Key:", there is a "File:" text input field with the pattern "*.PEM, *.DER, *.PVK" and a "Browse..." button. At the bottom is a "Password:" text input field. At the very bottom are "OK" and "Cancel" buttons.

Name: Define name for the object.

Public Key/Private Key: Select the file type for both public and private key and click **Browse** to select related file.

Password: Insert the password for the keys.

Authentication

The **Authentication** configuration module is used to set authentication methods for LAN users. Users defined on the equipment are LAN users who access network by using terminals. Users are basic units for allocating network permission. An administrator can manage users in a unified manner on the **Local Users** page and set authentication policies for LAN users on the **User Authentication** page.

Local Users

Overview

The firewall manages online users of terminals. Therefore, users are basic units for assigning network permission. An administrator can manage online users in a unified manner on the **Users** page.

Principle

3.7.1.2.1 User Authentication

Traditional network equipment is managed based on IP addresses. However, the NGAF equipment is managed based on users, increasing management convenience and accuracy compared with the equipment managed based on IP addresses.

To enable user-based management, the system must learn which user is using a certain IP address at a certain time point. Therefore, online users must be authenticated for enabling user-based management on network access behaviors.

The following types are available based on authentication methods:

1. User name/password

Before an online user of a terminal accesses the network, the browser is redirected to the authentication page, prompting the user to type the correct user name and password. Password authentication includes local password authentication and external server password authentication.

After an online user types the user name and password, the system checks whether the user name and password are correct in local user groups. If the user is not a local user and an external authentication server is configured, the system checks whether the user name and password are correct on the external authentication server.

Note that only accounts for which **Local password** is selected are applicable to local password authentication. If **Local password** is not selected, the user name and password are sent to the external authentication server.

2. SSO

SSO: If an authentication system is already configured on the network, the system can work together with the

authentication system to identify a user who is using a certain IP address. The user is not prompted to type the user name and password before accessing the network, reducing the impact on the online users.

At present, the following SSO types are supported:

SSO based on the MS Active Directory domain (see section 3.6.2.2.1.1)

SSO based on a proxy server (see section 3.6.2.2.1.2)

SSO based on a POP3 mail server (see section 3.6.2.2.1.3)

SSO based on web table authentication (see section 3.6.2.2.1.4)

3. Identification based on IP addresses, MAC addresses, and computer names

A user is identified based on the source IP address and source MAC address of data packets and the name of a computer used by the user. In this method, a user does not need to type the user name or password in the browser before accessing the network. Therefore, the user does not sense the existence of the equipment. However, the equipment cannot identify the specific name of the user either. Especially when IP addresses are dynamically identified, the equipment cannot associate network access behaviors with specific users, and therefore control cannot be exercised on specific users.

3.7.1.2.2 User Type

Users are classified into the following types based on user sources:

users automatically discovered and created by the equipment, users manually created by the administrator, users imported from .csv files, users imported from external LDAP servers, and users imported from computers on the network

Users are classified into the following types based on authentication methods:

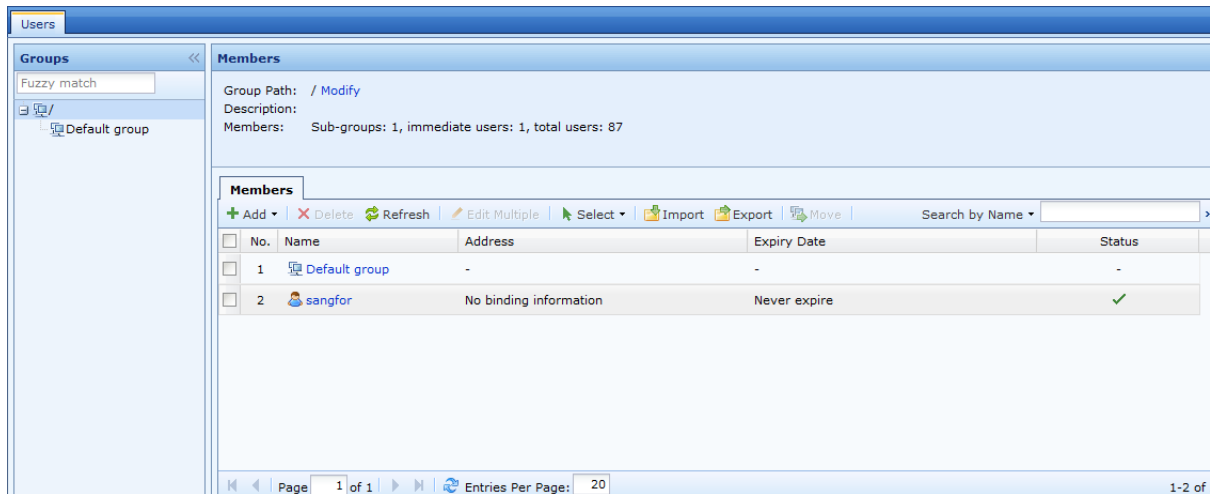
users who require no authentication (bound to IP addresses/MAC addresses), users who require local password authentication, users who require external password authentication, and SSO users (authenticated by the system together with an external authentication system)

Users

3.7.1.3.1 Viewing Users/Groups

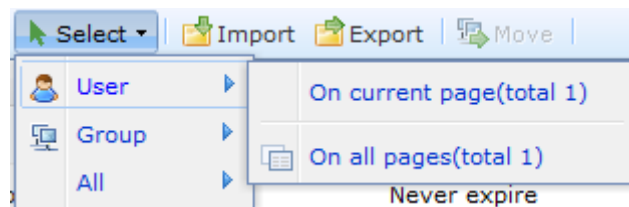
To view existing users and groups on the equipment, select a group in the **Groups** pane. The **Members** page on the right displays information of the group, including the group name, description, and detailed information.

Members: The **Members** page displays detailed information of sub-groups and users, including the group name, binding information (IP addresses and MAC addresses bound to the users), expiry date (for the users), description, and status (enabled or disabled). You can also select the information to be displayed by using the selection function.

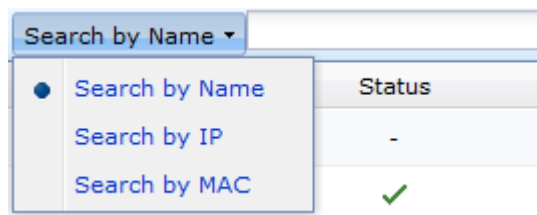


Selection function: This function is used to quickly select users and groups on the current page and on all pages.

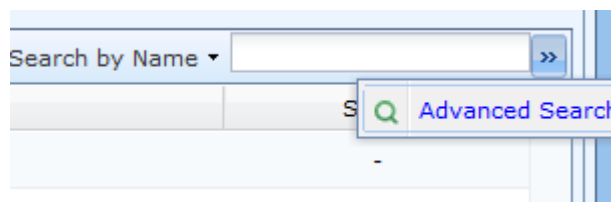
Click . The following page is displayed:



Search function: This function is used to quickly search for users or groups. Click the search box, select **Search by Name**, **Search by IP**, or **Search by MAC**, type information in the text box, and press **Enter**.



Advanced search: This function is only used to search for users. You can use this function to search for users based on multiple search criteria. Search criteria include basic search criteria and other search criteria. When you set multiple search criteria, they must be met at the same time.



The **Basics** pane displays three options, including **Username**, **IP**, and **MAC**. You can select only one of the three options. See the figure below:

Basics

☒ **Username**
Name:

☐ **IP**
Start IP:
End IP:

☐ **MAC**
MAC Address:

The Others pane displays three options, including Expiry Date, User Status, and Allow concurrent login on multiple terminals.

Others

☐ **Expiry Date**
Start Date:
End Date:

User Status: ☒ Any ☐ Enabled ☐ Disabled

☐ Allow concurrent login on multiple terminals

3.7.1.3.2 Adding Users/Groups

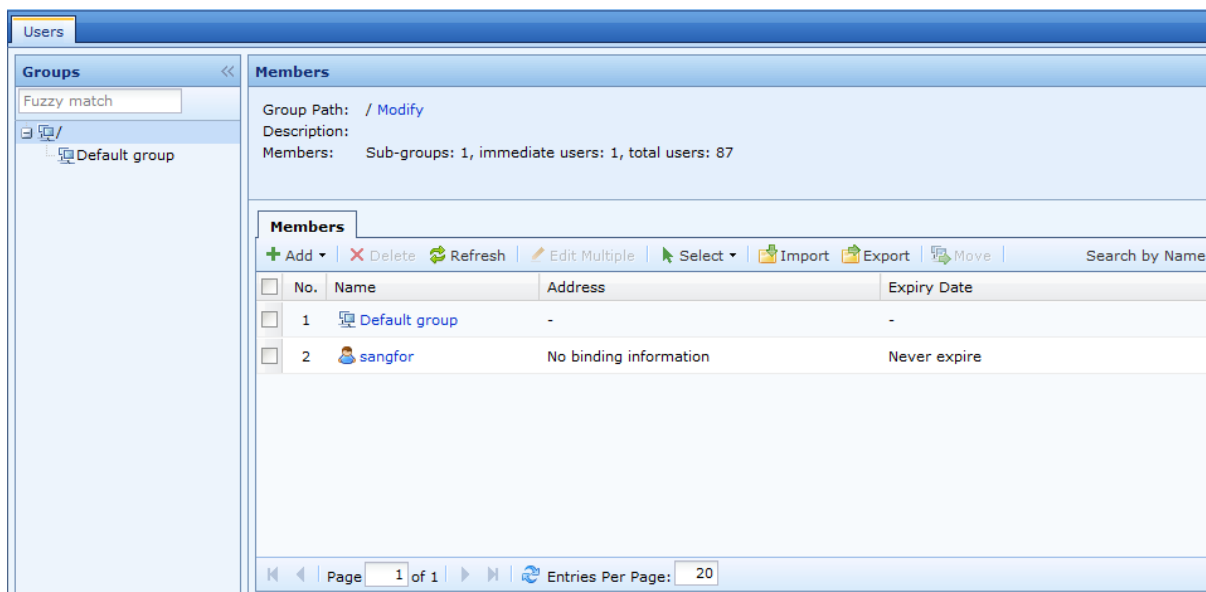
Adding Sub-groups

The default group on the equipment is the root group (indicated by a slash "/"). The root group cannot be deleted, and its group name cannot be modified. Groups created by users are sub-groups of the root group. Groups on the equipment are classified into different levels. The root group is a Level 1 group, sub-groups of the root group are Level 2 groups, and so on. This adapts to the organizational structure of an enterprise or an institution, thereby facilitating management.

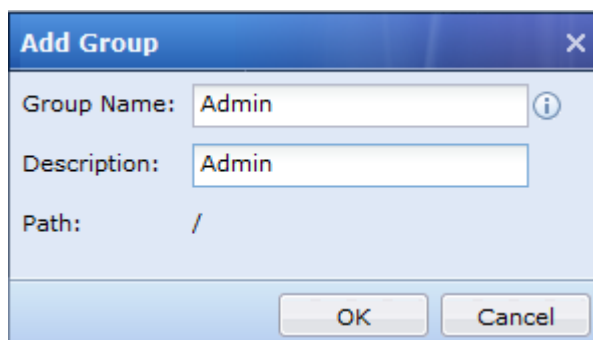
3.7.1.3.2.1 Configuration Example: Adding a Sub-Group

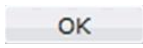
This section describes how to add an engineer sub-group under the root group.

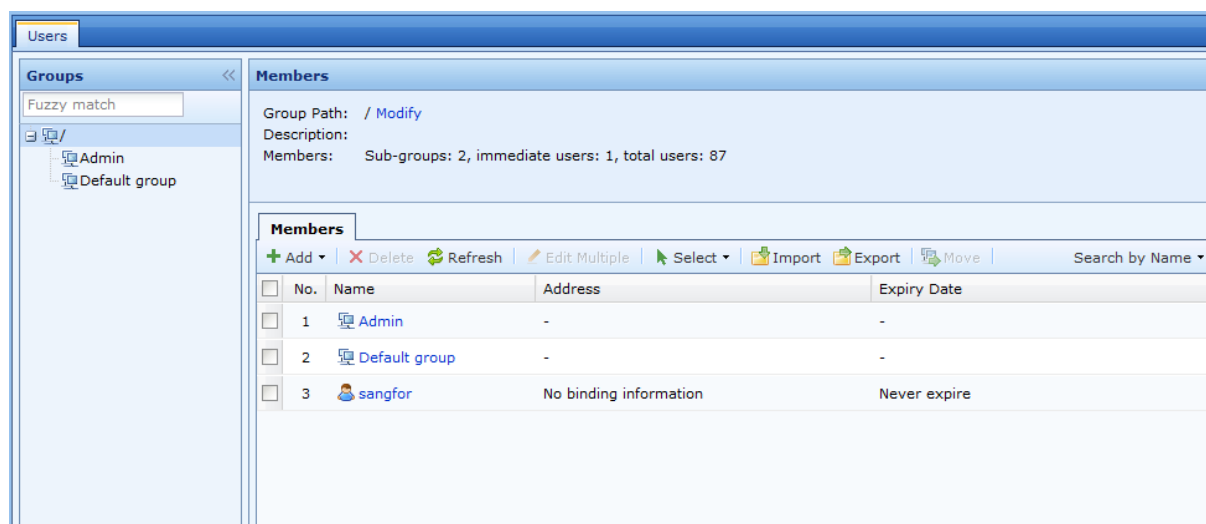
Step 1: In the **Groups** pane, select a group for which you want to add a sub-group. On the **Members** page displayed on the right, click **Add** and select **Group**.



Step 2: In the **Add Group** dialog box, type the group name in the **Group Name** text box, and type the group description in the **Description** text box.



Step 3: Click . The sub-group is added successfully.



The equipment supports a maximum of 16 levels of groups, including the root group.

Adding Users

You can add one or multiple users.

The following attributes need to be set for a new user: the user name, group name, password, and bound IP address/MAC address, excluding the authentication method. To set an authentication method for a LAN user, choose **User Authentication > Authentication Policy**, and set **IP/MAC Range** for the equipment to determine an authentication method for the user.

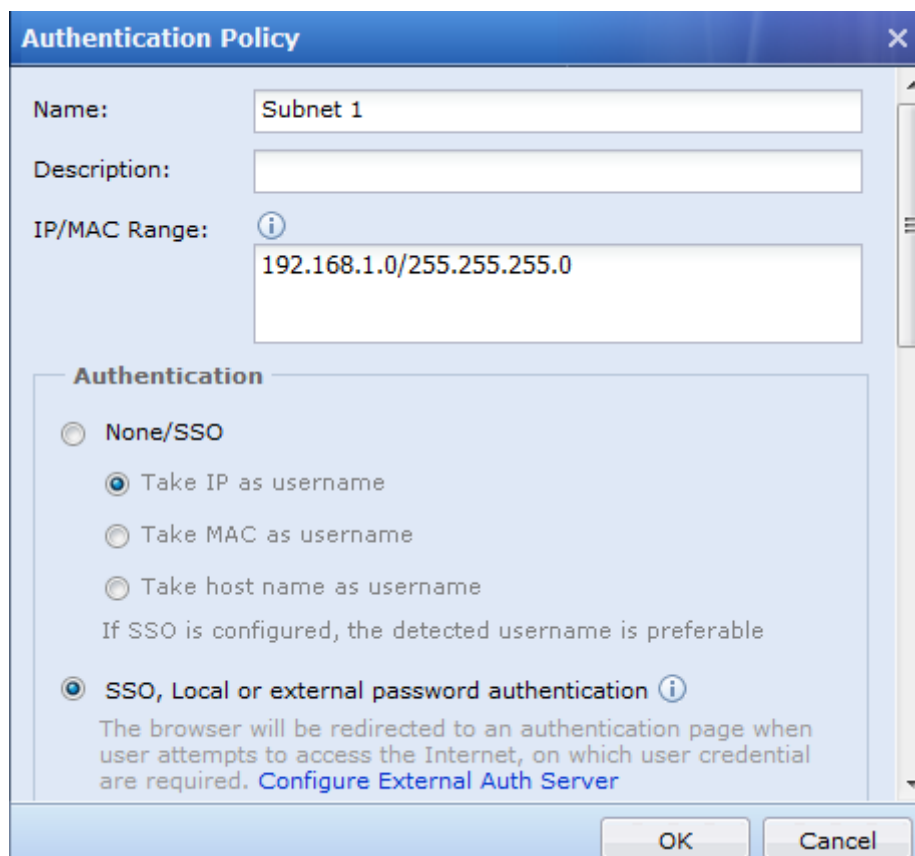
3.7.1.3.2.2 Configuration Example: Adding a User (1)

All computers on the network segment of 192.168.1.0/255.255.255.0 on the LAN of the customer are authenticated based on the user name and password. A public account needs to be added to the engineer group. The account is authenticated based on the user name and password and is bounded to an IP address range of 192.168.1.2–192.168.1.100 (IP address range available for login) in a unidirectional manner. This account can be used for concurrent login from multiple terminals.

Step 1: Configure an authentication method based on the user name and password for all computers on the network segment of 192.168.1.0/255.255.255.0. First, set an authentication method for all users on the network segment.

Choose **User Authentication > Authentication Policy**. In the **Authentication Policy** dialog box, set **IP/MAC Range**, and set **Authentication** to **SSO, Local or external password authentication**. Before you set **Authentication Policy**, set **Authentication Zone**. As shown in the figure below, the LAN is selected for authentication. For details about the settings, see section 4.2.1.4.





Authentication Policy

Name: Subnet 1

Description:

IP/MAC Range: 192.168.1.0/255.255.255.0

Authentication

☐ None/SSO

- ☒ Take IP as username
- ☐ Take MAC as username
- ☐ Take host name as username

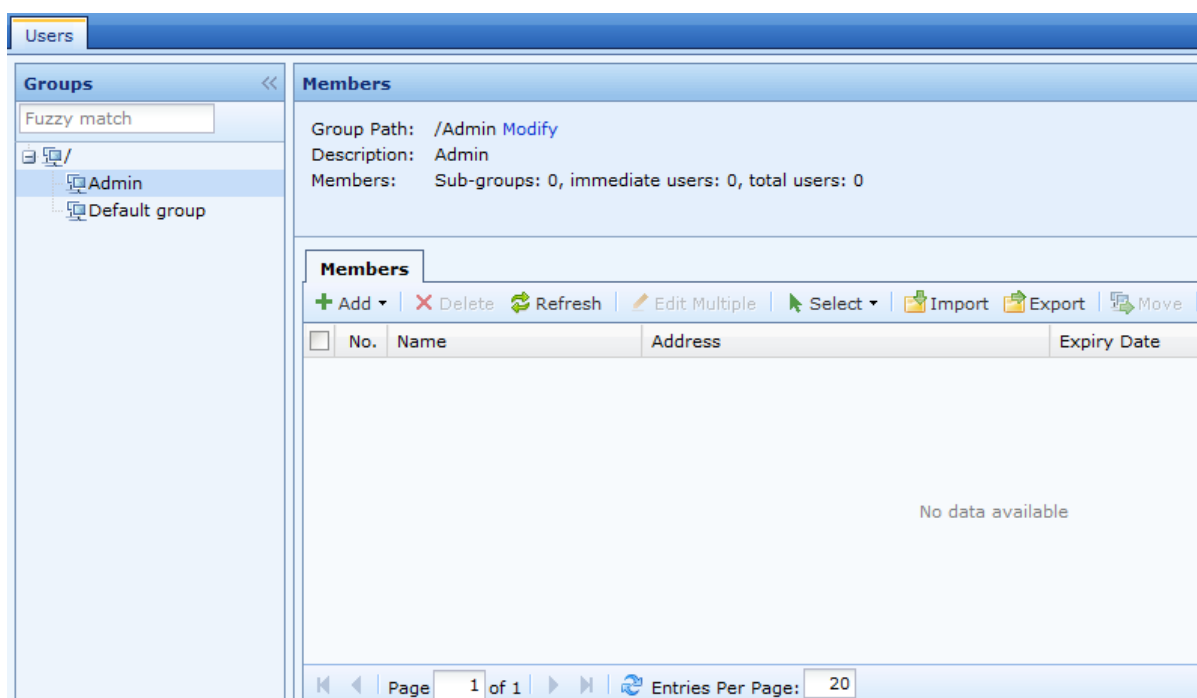
If SSO is configured, the detected username is preferable

☒ SSO, Local or external password authentication

The browser will be redirected to an authentication page when user attempts to access the Internet, on which user credential are required. [Configure External Auth Server](#)

OK Cancel

Step 2: In the **Groups** pane, select a group for which you want to add a user. On the **Members** page displayed on the right, click **Add** and select **User**.



Users

Groups

Fuzzy match

- /
- Admin
- Default group

Members

Group Path: /Admin [Modify](#)

Description: Admin

Members: Sub-groups: 0, immediate users: 0, total users: 0

Members

+ Add - Delete Refresh Edit Multiple Select Import Export Move

No.	Name	Address	Expiry Date
No data available			

Page 1 of 1 Entries Per Page: 20

Step 3: In the **Add User** dialog box, select **Enable user**, and set **Name**, **Description**, **Display Name**, and **Added To Group**.

Add User

☒ Enable user

Name:

Description:

Display Name:

Added To Group:

Step 4: Set **User Attributes**. The **User Attributes** settings include the authentication method, public account, and expiry date.

Select **Local password**, and type the password for login authentication in the **Password** text box.

☒ Local password ⓘ

Password:

Confirm:

Select **Bind IP/MAC**, and bind the user to IP addresses and MAC addresses. In this example, bind the user to an IP address range of 192.168.1.2–192.168.1.100 (IP address range available for login) in a unidirectional manner.

Click **Binding Mode**, and select **Unidirectional binding between user and address** in the displayed dialog box.

Select **IP Address**, and type **192.168.1.2-192.168.1.100** in the text box.

☒ Bind IP/MAC: [Binding Mode](#)

☒ IP Address ⓘ ☐ MAC Address ⓘ ☐ IP and MAC ⓘ

One entry per row. Annotation is separated by #. Example: #200.200.0.1

The **Allow concurrent login on multiple terminals** option is used to set whether multiple users can log in by using the account at the same time. If you select this option, multiple users can log in by using the account at the same time. In this example, select **Allow concurrent login on multiple terminals**.

☒ Allow concurrent login on multiple terminals ⓘ

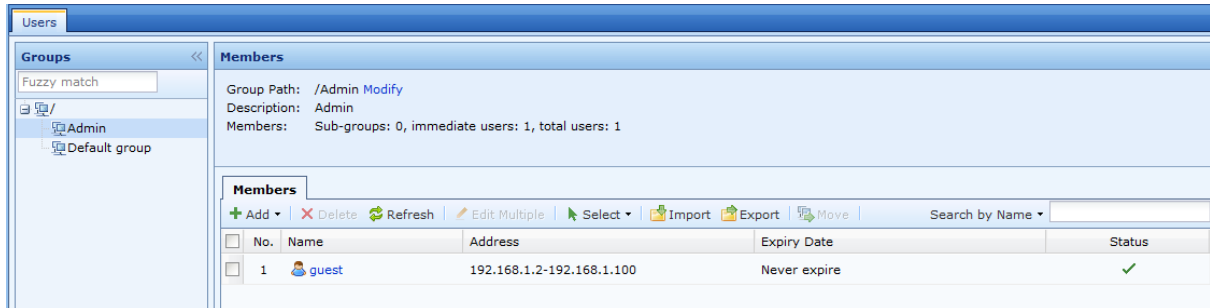
Select **Show Logout page if user passes password based authentication**. This option is available for users authenticated based on the user name and password. If this option is selected, the logout page is displayed after successful login.

☐ Show Logout page if user passes password based authentication

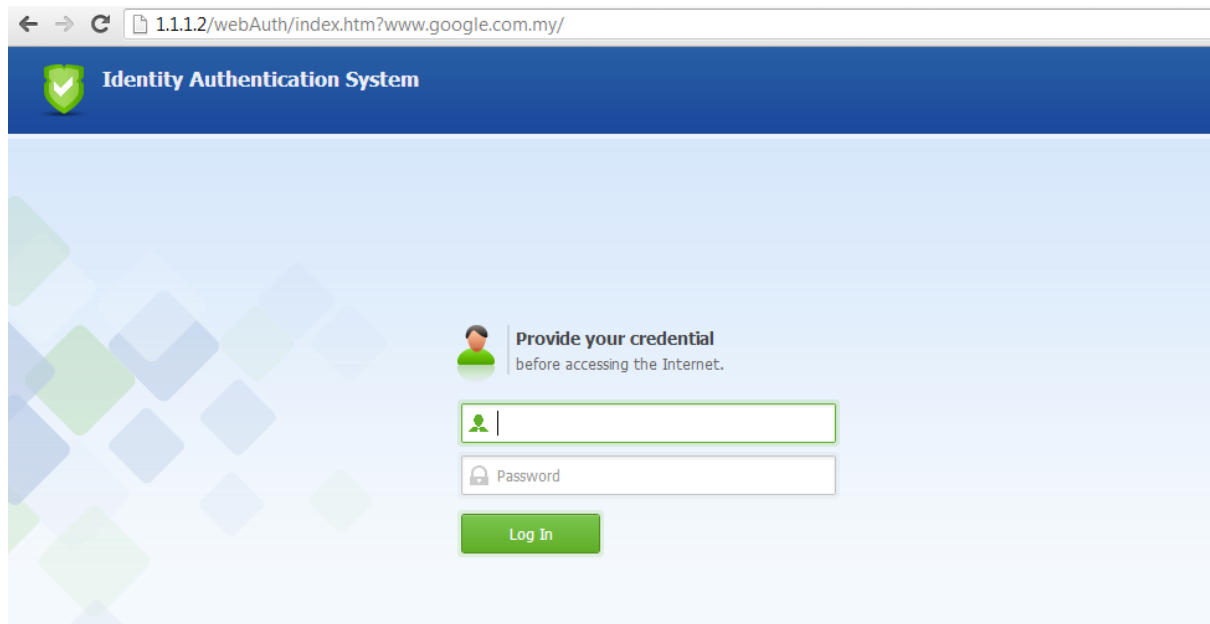
Set **Expiry Date** for the user.

Expiry Date: ☒ Never expire
☐ Date

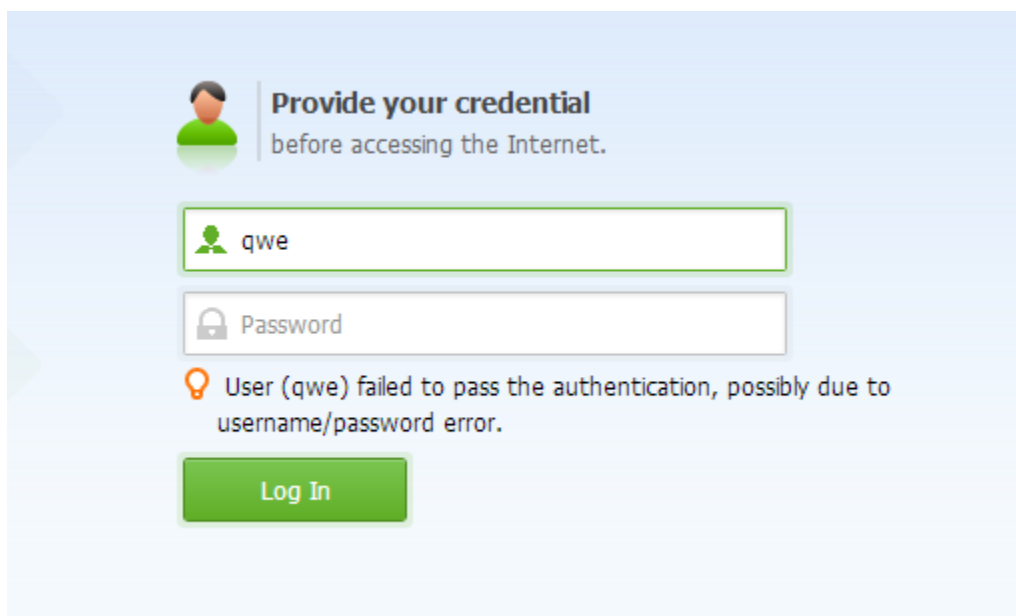
Step 5: After the user attributes are set properly, click **OK**. The user is added successfully.



Step 6: Open a webpage as a user on the corresponding network segment. The webpage is redirected to the authentication page of the equipment. Type the user name and password, and click **Log In**. If the user name and password are correct and meet the bound IP address range, the authentication is successful.



If the user name and password are correct, but the IP address used for login is beyond the bound IP address range, the authentication fails, and a reminder message is displayed. See the figure below:



Two binding modes are available for Bind IP/MAC: **unidirectional binding** and **bidirectional binding**.

Unidirectional binding: A user can use only a specified IP address for authentication, and other users can also use the specified IP address for authentication.

Bidirectional binding: A user can use only a specified IP address for authentication, and the specified IP address is only available for the user.

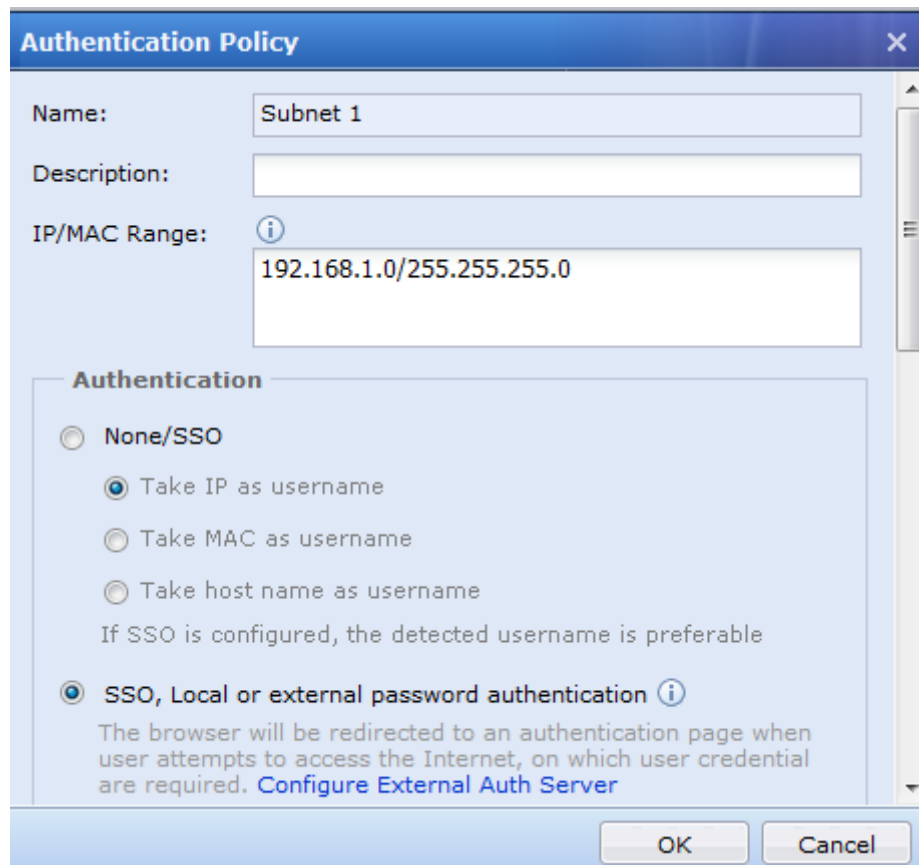
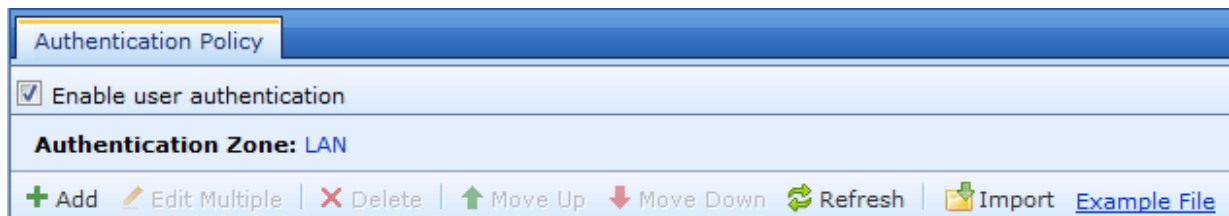
In the example, the created user is authenticated based on the user name and password and is bound to IP addresses in a unidirectional manner. The following example describes how to add a user bound to IP addresses in a bidirectional manner.

3.7.1.3.2.3 Configuration Example: Adding a User (2)

All computers on the network segment of 192.168.1.0/255.255.255.0 on the LAN of the customer are authenticated based on the user name and password. A user named Engineer Li needs to be added to the engineer group. The user is authenticated based on the user name and password and is bounded to the IP address/MAC address of 192.168.1.117/00-1C-25-AC-4C-44 (IP address/MAC address required for authentication and unavailable for other users).

Step 1: Configure an authentication method based on the user name and password for all computers on the network segment of 192.168.1.0/255.255.255.0. First, set an authentication method for all users on the network segment.

Choose **User Authentication > Authentication Policy**. In the **Authentication Policy** dialog box, set **IP/MAC Range**, and set **Authentication** to **SSO, Local or external password authentication**. Before you set **Authentication Policy**, set **Authentication Zone**. As shown in the figure below, the LAN is selected for authentication.



Step 2: In the **Groups** pane, select a group for which you want to add a user. On the **Members** page displayed on the right, click **Add** and select **User**.



Step 3: In the **Add User** dialog box, Select **Enable user**, and set **Name**, **Description**, **Display Name**, and **Added To Group**.

Step 4: Set **User Attributes**. Select **Local password**, and type the password for login authentication in the **Password** text box.

Select **Bind IP/MAC**, and bind the user to IP addresses and MAC addresses. In this example, bind the user to the IP address/MAC address of 192.168.1.117/00-1C-25-AC-4C-44 (IP address/MAC address required for authentication and unavailable for other users) in a bidirectional manner.

Click **Binding Mode**, and select **Bidirectional binding between user and address** in the displayed dialog box.

Select **Bind IP/MAC**, and type **192.168.1.117(00-1C-25-AC-4C-44)** in the text box.

The user is bound only to one IP address and one MAC address. Therefore, the user is identified as a private account by default.

Select **Show Logout page if user passes password based authentication**. This option is available for users authenticated based on the user name and password. If this option is selected, the logout page is displayed after successful login.

Set **Expiry Date** for the user.

Expiry Date: ☒ Never expire
☐ Date

Step 5: After the user attributes are set properly, click **OK**. The user is added successfully.

Groups
Fuzzy match
Admin
Default group

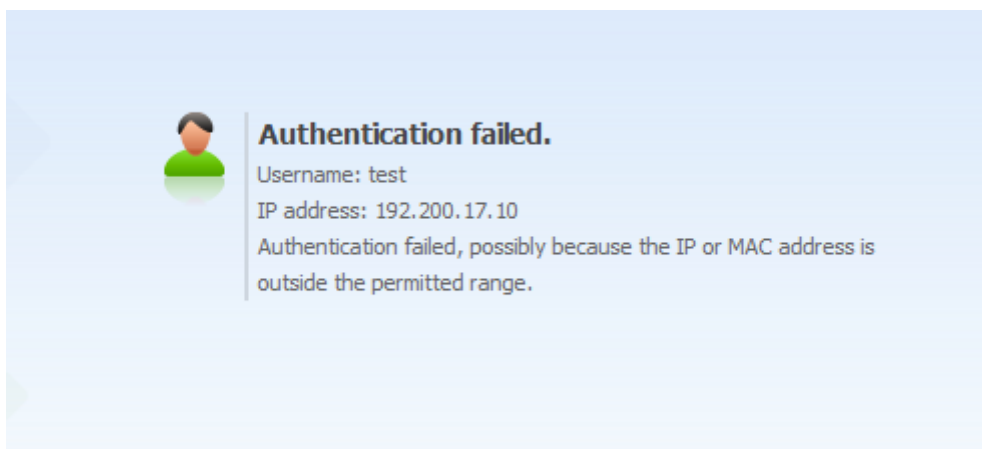
Members
Group Path: /Admin Modify
Description: Admin
Members: Sub-groups: 0, immediate users: 2, total users: 2

Members
Add Delete Refresh Edit Multiple Select Import Export Move Search by Name

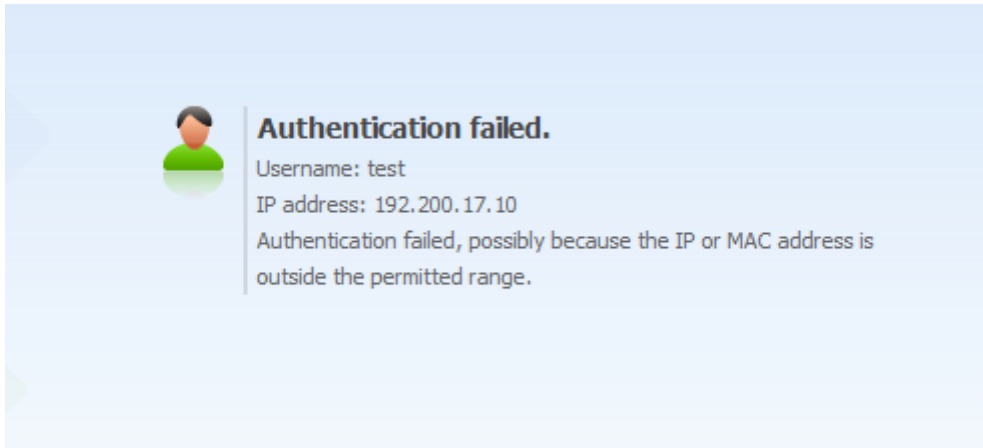
No.	Name	Address	Expiry Date
1	guest	192.168.1.2-192.168.1.100	Never expire
2	test	192.168.1.117(00-1c-25-ac-4c-44)	Never expire

Step 6. Open a webpage as a user on the corresponding network segment. The webpage is redirected to the authentication page of the equipment. Type the user name and password, and click **Log In**. If the user name and password are correct and meet the bound IP address, the authentication is successful.

If the user name and password are correct, but the IP address/MAC address used for login are inconsistent with the bound IP address/MAC address, the authentication fails, and a reminder message is displayed. See the figure below:



Authentication for other users using the IP address/MAC address also fails.



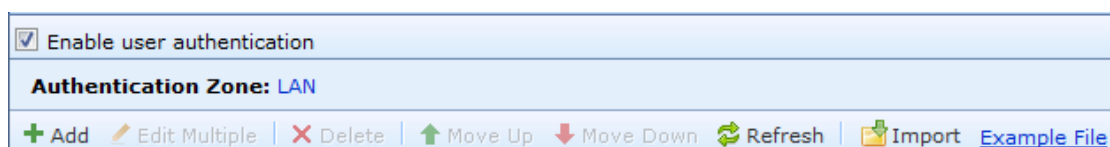
Choose **User Authentication > Authentication Policy**. In the **Authentication Policy** dialog box, if users using certain IP addresses do not need to be authenticated, they can access the network without typing the user name or password. In this case, the equipment identifies the users based on IP addresses, MAC addresses, and computer names. General settings are as follows:

1. When you create a user, bind the user to an IP address and a MAC address in a bidirectional manner. In this case, the IP address/MAC address are in a one-to-one mapping with the user, so the equipment can identify the user based on the IP address and MAC address.
2. Choose **User Authentication > Authentication Policy**. In the dialog box, deselect **Enable user authentication**, and use the IP address, MAC address, or computer name as the user name. When a LAN user is authenticated, the LAN user is matched to the corresponding user name based on the IP address, MAC address, or computer name.

3.7.1.3.2.4 Configuration Example: Adding a User (3)

A user named **Manager** needs to be added to the **/Engineer** group. The user does not need to be authenticated and is bound to the IP address/MAC address of the manager's computer in a bidirectional manner. Therefore, the account can be used only on the manager's computer. The IP address/MAC address of the manager's computer are 192.168.1.117(00-1C-25-AC-4C-44).

Step 1. Choose **User Authentication > Authentication Policy**. In the **Authentication Policy** dialog box, set **IP/MAC Range**, and set **Authentication** to **None/SSO**. Before you set **Authentication Policy**, set **Authentication Zone**. As shown in the figure below, the LAN is selected for authentication.



Authentication Policy

Name:

Description:

IP/MAC Range:

Authentication

☒ None/SSO

- ☒ Take IP as username
- ☐ Take MAC as username
- ☐ Take host name as username

If SSO is configured, the detected username is preferable

☐ SSO, Local or external password authentication ⓘ

The browser will be redirected to an authentication page when user attempts to access the Internet, on which user credential are required. Configure External Auth Server

☐ SSO only ⓘ

Excluded Users:

New User Option (for users outside local device)

☒ Added to specified local group

Select Group:

OK Cancel

Step 2: In the **Groups** pane, select a group for which you want to add a user. On the **Members** page displayed on the right, click **Add** and select **User**.

Users

Groups

Fuzzy match

- /
- Default
- test

Members

Group Path: /Default/test Modify

Description: test

Members: Sub-groups: 0, immediate users: 1, total users: 1

Members

+ Add - Delete Refresh Edit Multiple Select Import Export Move Search by Name

No.	Name	Address	Expiry Date	Status
1	usera	No binding information	Never expire	✓


Step 3: In the **Add User** dialog box, Select **Enable user**, and set **Name**, **Description**, **Display Name**, and **Added To Group**.

☒ Enable user

Name:

Description:

Display Name:




Added To Group: 

Step 4: Set **User Attributes**. Select **Bind IP/MAC**, and bind the user to the IP address/MAC address. In this example, bind the user to the IP address/MAC address of 192.168.1.117/00-1C-25-AC-4C-44 in a bidirectional manner.

Click **Binding Mode**, and select **Bidirectional binding between user and address** in the displayed dialog box.

Select **Bind IP/MAC**, and type **192.168.1.117(00-1C-25-AC-4C-44)** in the text box.

☒ Bind IP/MAC: [Binding Mode](#)

☐ IP Address  ☐ MAC Address  ☒ IP and MAC 

One entry per row. Annotation is separated by #. Example: #200.200.0.1

Set **Expiry Date** for the user.

Expiry Date: ☒ Never expire

☐ Date

Step 5: After the user attributes are set properly, click **OK**. The user is added successfully.

Groups		Members			
Fuzzy match		Group Path: /Admin Modify			
<div> <div></div> <div>/</div> <div>Admin</div> <div>Default group</div> </div>		Description: Admin			
		Members: Sub-groups: 0, immediate users: 3, total users: 3			
		Members			
		+ Add X Delete Refresh Edit Multiple Select Import Export Move			
No.	Name	Address		Expiry Date	
1	guest	192.168.1.2-192.168.1.100		Never expire	
2	manager	192.168.1.217(00-1c-25-ac-4c-12)		Never expire	
3	test	192.168.1.117(00-1c-25-ac-4c-44)		Never expire	

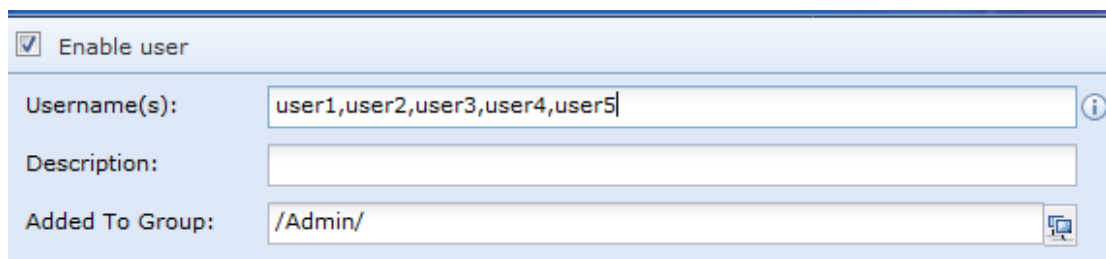
Step 6: Access the network on the equipment to verify the IP address/MAC address. If the IP address/MAC address are correct, the authentication is successful, and the authentication page is not displayed.

If the IP address/MAC address are inconsistent with the bound IP address/MAC address, the authentication fails, no reminder message is displayed, and the client fails to connect to the network.

Adding Multiple Users

You can add multiple users at a time. In this case, the bidirectional binding mode for **Bind IP/MAC** is unavailable when you set user attributes for multiple users, because the bidirectional binding mode is unique.

When you add multiple users at a time, the attributes and policies of the users are the same, except the user names. Type multiple user names in the **Username(s)** text box, and separate them by commas. For details about other settings, see the process for adding a single user.



☒ Enable user

Username(s):

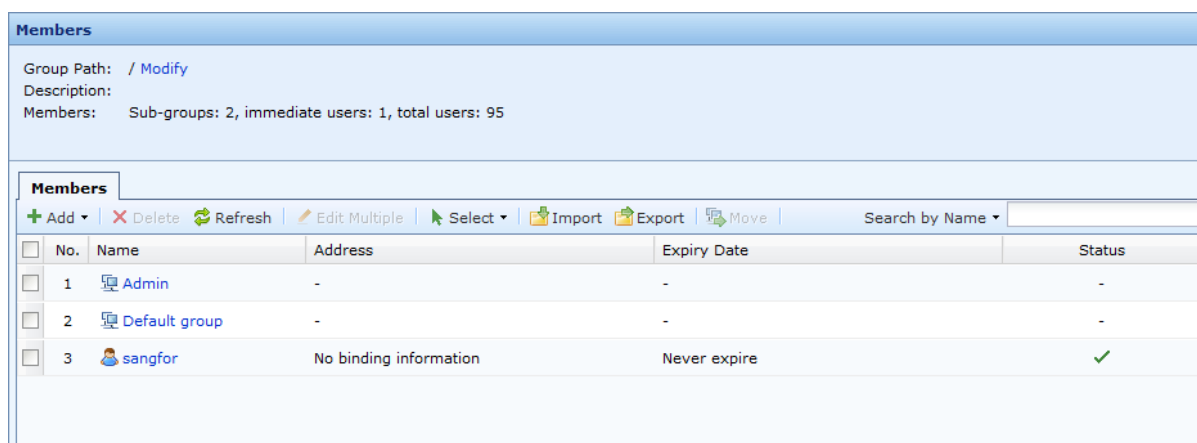
Description:

Added To Group:

Deleting Users/Groups

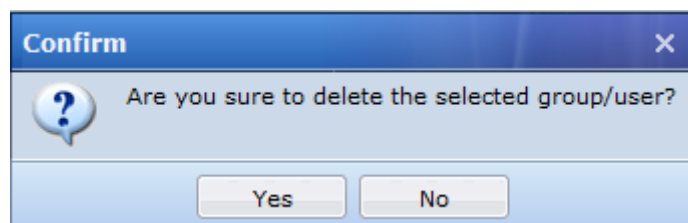
You can delete users or groups as required by using this function.

Step 1: Select a group or a user.



No.	Name	Address	Expiry Date	Status
1	Admin	-	-	-
2	Default group	-	-	-
3	sangfor	No binding information	Never expire	✓

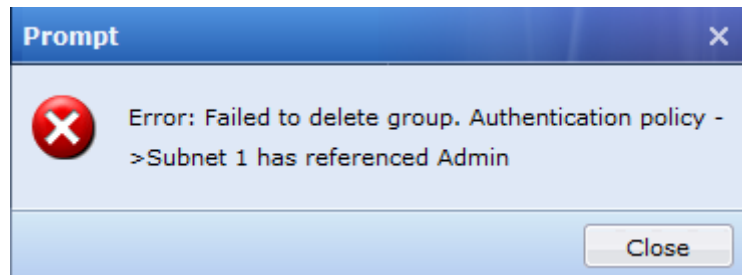
Step 2: Click **Delete**.



Step 3: Click **Yes**. The selected group or user is deleted. Deletion success information is displayed on the console.



If the group to be deleted is associated with a policy set in the Authentication Policy dialog box, the group fails to be deleted, as shown in the figure below. In this case, delete the associated policy from the Authentication Policy dialog box. (For details about authentication policy settings, see section 3.6.2.1.)



3.7.1.4.1 Editing Users/Groups in Batches

Attributes available when you edit users or groups in batches are different from those available when you edit a single user or group. You can edit multiple users or groups at a time. In this case, the bidirectional binding mode is unavailable for **Bind IP/MAC**, because batch editing and bidirectional binding are mutually exclusive.

3.7.1.4.1.1 Configuration Example: Editing Users/Groups in Batches

Set **Description** to **Engineering Department** for users **guest**, **test**, **user1**, **user2**, **user3**, and **user4**. Set the same password for the users, bind the users to an IP address range of 192.168.1.1-192.168.1.255 in a unidirectional manner, and set the expiry date for the users to January 1, 2012.

Step 1: Select users **guest**, **test**, **user1**, **user2**, **user3**, and **user4**, and click **Edit Multiple**.

Members					
<div><div>+ Add</div><div>✖ Delete</div><div>🔄 Refresh</div><div>✎ Edit Multiple</div><div>👉 Select</div><div>📁 Import</div><div>📄 Export</div><div>📁 Move</div></div> <div>Search by Name</div>					
<input type="checkbox"/>	No.	Name	Address	Expiry Date	Status
<input checked="" type="checkbox"/>	1	guest	192.168.1.2-192.168.1.100	Never expire	✓
<input type="checkbox"/>	2	manager	192.168.1.217(00-1c-25-ac-4c-12)	Never expire	✓
<input checked="" type="checkbox"/>	3	test	192.168.1.117(00-1c-25-ac-4c-44)	Never expire	✓
<input checked="" type="checkbox"/>	4	user1	No binding information	Never expire	✓
<input checked="" type="checkbox"/>	5	user2	No binding information	Never expire	✓
<input checked="" type="checkbox"/>	6	user3	No binding information	Never expire	✓
<input checked="" type="checkbox"/>	7	user4	No binding information	Never expire	✓

Step 2: Select **Description** and type **Engineering Department**. Select **Password Settings** and **Local password**, and type the password.

Edit Multiple Users

User Attributes

Username:

☐ User Status

☒ Enable

☐ Disable

☒ Description

☒ Password Settings

☒ Local password

Password:

Confirm:

Step 3: Select **Bind IP/MAC** and **Enable IP/MAC Binding**. Select **Modify IP/MAC address** and type **192.168.1.1–192.168.1.255**. Select **Expiry Date** and **Date**, and set the date to **2012-01-01 00:00**.

SANGFOR NGAF 6.4 User Manual

177

☒ **Bind IP/MAC**

☒ **Enable IP/MAC Binding**

☐ Bidirectional binding between user and address
☒ Unidirectional binding between user and address

☒ **Modify IP/MAC address**

☒ IP Address
☐ MAC address
☐ IP/MAC address

Required. One IP range per row. Login is allowed on those addresses only.

192.168.1.1-192.168.1.255

Obtain Mappings from IP Group
Scan MAC

☐ **Public Account**

☐ Allow concurrent login on multiple terminals ⓘ

☐ **Logout Page**

☐ Show Logout page if user passes password based authentication


☒ **Expiry Date**

☒ Never expire
☐ Date

Step 4: Click **OK**. The batch editing is completed.

3.7.1.4.2 Importing and Exporting Users/Groups

You can import users or groups in or export them from the equipment in batches by using this function.

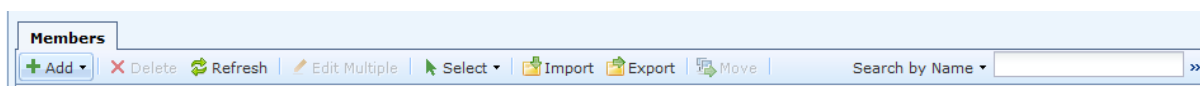
Click  and select **Import**. The **User Import** page is displayed. You can import users on this page. For details, see section 3.6.1.4.

3.7.1.4.2.1 Configuration Example: Exporting Users/Groups

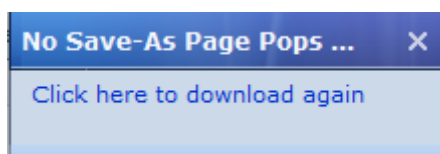
Export the **Engineering Department** group and the users.

Step 1: On the **Members** page, select the **Engineering Department** group, click , and

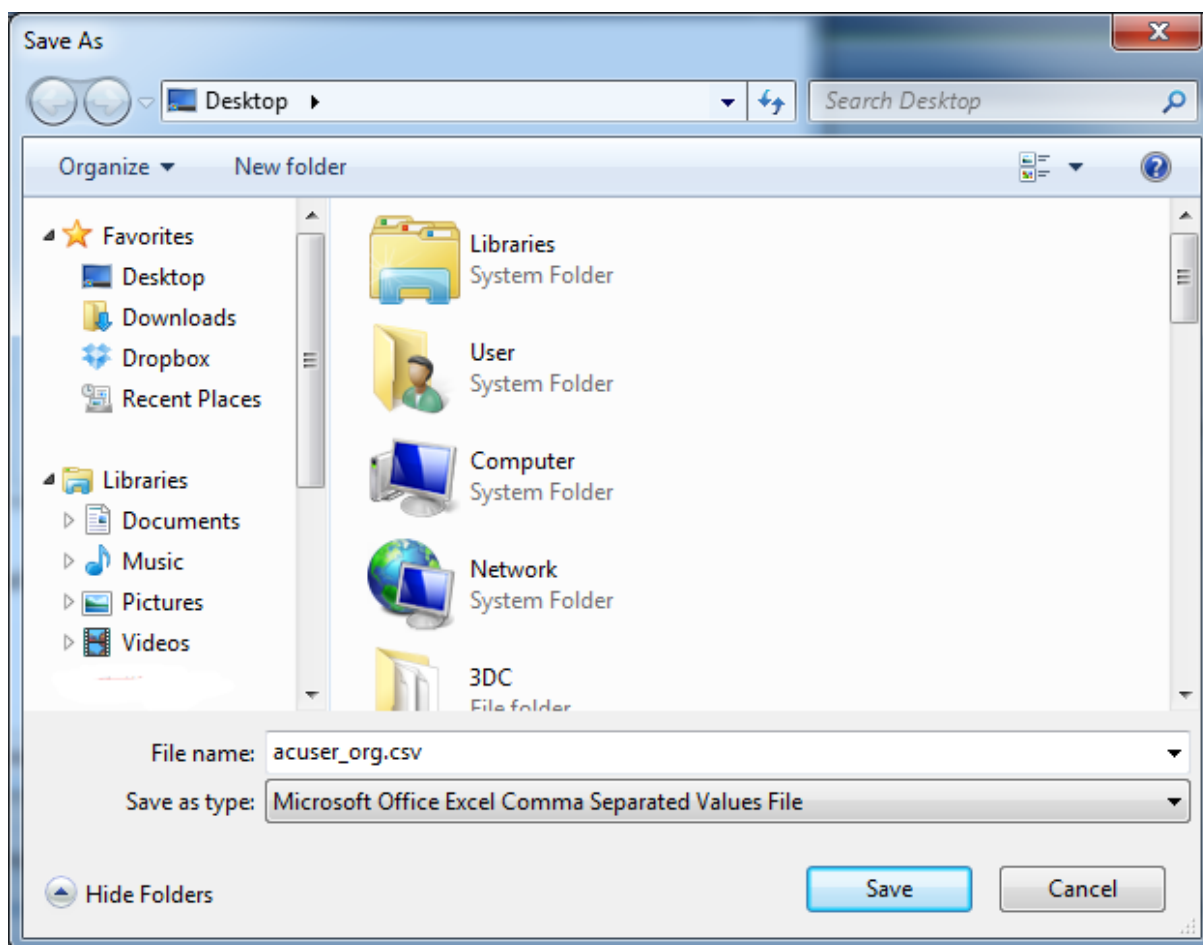
select **Export**.



Step 2: Check the export success information on the console, and click the link in the displayed dialog box.



Step 3: Save the exported file. The **Engineering Department** group and the users are exported successfully.



If a group contains no users, the group cannot be exported independently.

3.7.1.4.3 Moving Users/Groups

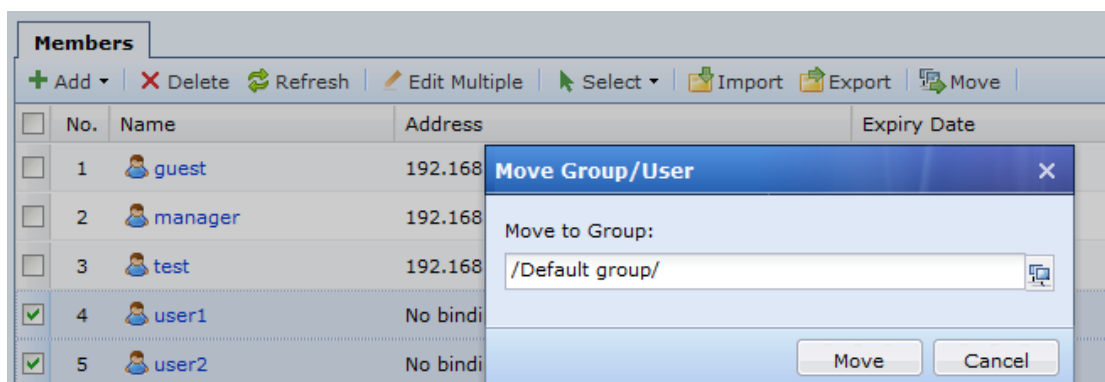
You can move an existing user or group to another group. After the operation is successful, the user or group is moved to the target group.

3.7.1.4.3.1 Configuration Example: Moving Users/Groups

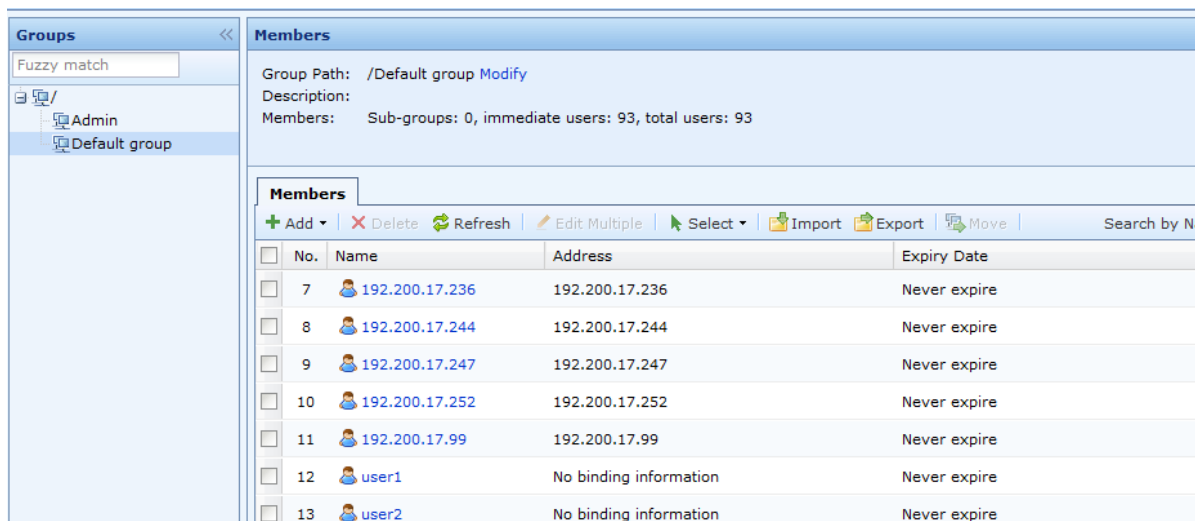
Move **user1** and **user2** to **/Default group**.

Step 1: Select **user1** and **user2**, click **Move**, and select a target group.

Click **Move**. **user2** is moved successfully.



Step 2: Click **Move**. **user1** and **user2** are moved successfully. No further operation is required.



A common administrator can manage only certain groups. Therefore, a common administrator cannot move a user or a group to another group beyond the permission of the common administrator.

User Import

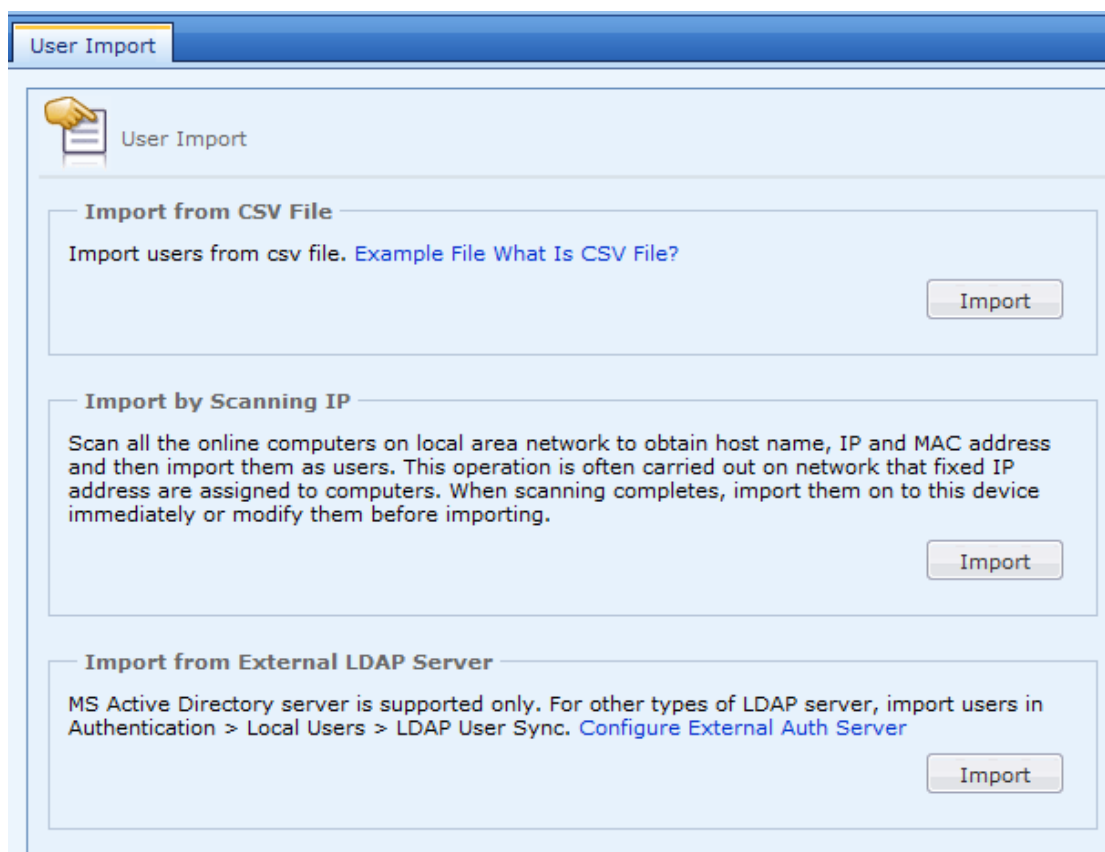
You can import users in batches in the following three methods:

Import from CSV File: You can import users from a CSV file, including user information such as the user names, authentication methods, IP/MAC address binding information, and passwords. If the target group for importing the users does not exist, a group is automatically created during the import.

Import by Scanning IP: When you import users bound to IP addresses/MAC addresses, you can scan MAC

addresses of LAN users by using this method, facilitating user import. In this method, users are imported in the root group by default and do not need to be authenticated. The bound IP addresses/MAC addresses and the user names are the computer names obtained by scanning. If the imported IP address conflicts with the bound IP address of a user, the user cannot be imported.

Import from External LDAP Server: You can synchronize users from an LDAP server to the equipment. For example, you can import users from the MS Active Directory server. When you import domain users by using this method, security groups on the domain server are imported in the equipment, and users are imported in the corresponding security groups.



3.7.1.5.1 Import from CSV File

You can import users from a CSV file, including user information such as the user names, authentication methods, IP/MAC address binding information, and passwords. If the target group for importing the users does not exist, a group is automatically created during the import.

A CSV file is in a simple format and can be edited and stored by most spreadsheet software. For example, Microsoft Excel can edit CSV files and easily convert XLS files into CSV files. CSV files do not support column width, font, or color settings. Therefore, to facilitate user editing and management, you can edit user information in XLS files and convert the XLS files into CSV files before import.

Import from CSV File

Import users from csv file. [Example File](#) [What Is CSV File?](#)

Import

Step 1: Click **Example File** to download example user information. Set the user information that you want to import based on the format in the example file.

	A	B	C	D	E	F	G	H	I	J	K	L
1	# The line	no need to be filled with value.										
2	# Please refer to the example below to enter the accounts to be imported. "" indicates that the field is required. Please DO NOT											
3	# Local Password: being left blank means the password is null; N/A indicates the user is not configured with local password and s											
4	# Bind IP (Unidirectional): being left blank indicates that the user can log in with any IP address. Multiple addresses are supporte											
5	# Bind IP (Bidirectional): being left blank indicates that the user can log in with any IP address. Multiple addresses are supported											
6	# Allow Multi-User Login: filled with Y or N; being left blank means N.											
7	# Enable Account: filled with Y or N; being left blank means Y.											
8	# Expiry Time: format is ""yy-mm-dd hh:mm""; being left blank indicates that the account will never get expired."											
9	Login Name/Display Name/Group Path/Description/Local Password/Bind IP (U/Bind IP (B/Allow Multi-User Login/Enable Account/Expiry Time											
10	Zhang Shan	/HQ/Mark	New member	password								
11	Li Si	/HQ/RD/	Local password is null	10.0.10.10			N		N			
12	ID_95471	Wang Wu	/Default group	No local password	N/A	10.0.1.0-10.0.1.255,1	Y		Y			
13	Zhao Liu	/Default group/	password	00-A1-B2-C3-D4-E5,0	Y			Y				
14	Qian Qi	/Default group/	123	10.0.0.2(00-A1-B2-C3-D4-E5)	Y			Y		#####		
15	Mail Server	/Server		N/A		10.0.0.1	N			#####		

Step 2: Import the CSV file: Click **Import**. In the **Import CSV File** dialog box, select the file that you want to import, and select **If user group does not exist, create it**. If the target group for importing the users does not exist, the equipment automatically creates a group during the import. If the **If user group does not exist, create it** option is deselected, the equipment does not create a group during the import, and instead, the users are imported in the root group. Select **Proceed and overwrite existing one** under **If user already exists**. If users with the same user names already exist in the user list, attributes of the users are updated. Or you can select **Skip and not overwrite existing user**. In this case, if users with the same user names already exist in the user list, attributes of the users are not updated, and the users are not imported.

Import CSV File

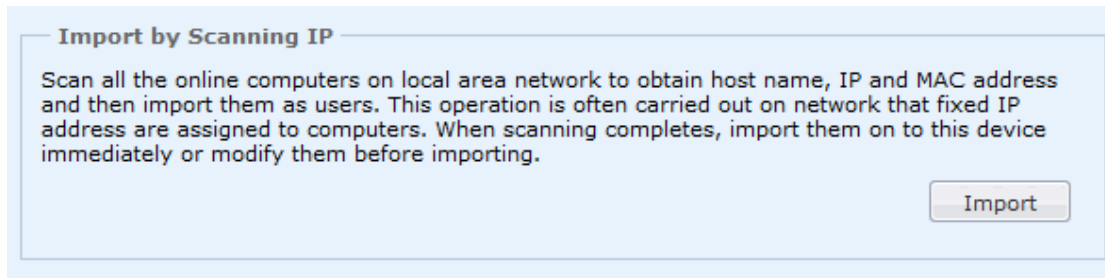
☒ If user group does not exist, create it

If user already exists:

☒ Proceed and overwrite existing one
 ☐ Skip and not overwrite existing user

3.7.1.5.2 Import by Scanning IP

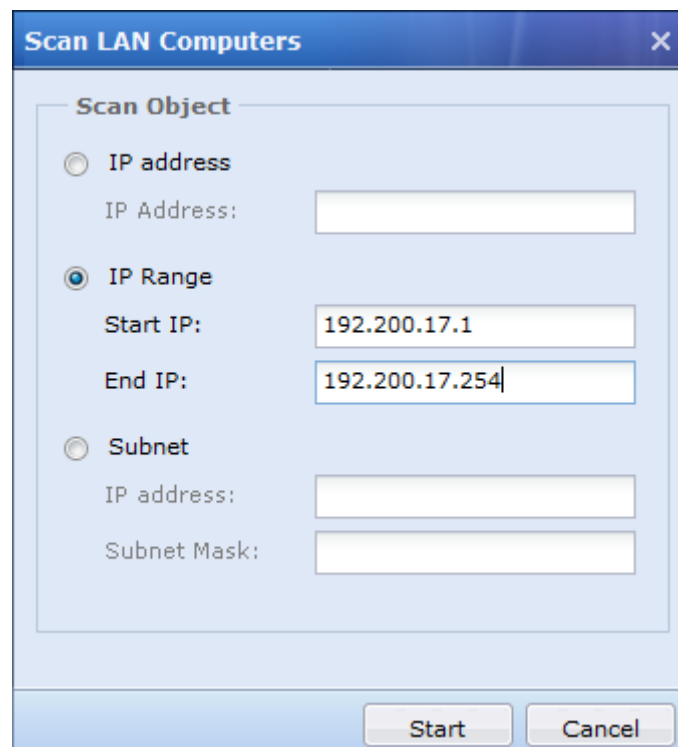
You can scan IP addresses and MAC addresses, and import identified users in the equipment. The computer names obtained by scanning are used as the user names. The users are imported in the root group by default and are bounded to IP addresses and MAC addresses, but do not need to be authenticated.



3.7.1.5.2.1 Configuration Example: Import by Scanning IP

Scan computers on the network segment of 192.200.200.1–192.200.200.100 on the LAN, and import them in the user list.

Step 1: Select **Import by Scanning IP**, click **Import**, and type the IP address range that you want to scan.



Step 2: Click **Start**. Computers on the network segment of 192.200.17.1–192.200.17.254 are displayed. Only survived computers are identified. **Username** displays the computer names.

Preview Scanning Result			
No.	Username	IP Address	MAC Address
1	ERIC-PC	192.200.17.11	4c-ed-de-a2-9c-a6
2	DELL-LIM	192.200.17.12	60-6c-66-42-e9-74
3	SUPPORT-SERVER	192.200.17.31	00-0c-29-48-e6-3c
4	KT-PC	192.200.17.99	8c-89-a5-ff-43-55
5	ANDY	192.200.17.111	a4-17-31-f6-b4-fc
6	RICHARD-PC	192.200.17.114	60-67-20-78-84-c2
7	SUPPORT-SERVER-	192.200.17.117	00-0c-29-e2-a6-86
8	TONY-LAPTOP	192.200.17.118	00-24-d7-46-39-28
9	USER-PC	192.200.17.124	8c-a9-82-bf-14-b8
10	SANGFOR-PC	192.200.17.125	e4-d5-3d-97-7f-d9
11	VIRUS-PC	192.200.17.131	e4-d5-3d-c1-50-b7
12	CARMENPC	192.200.17.133	bc-ae-c5-6f-42-83
13	BRW00225853BD...	192.200.17.202	00-22-58-53-bd-17
14	TEAMV	192.200.17.223	00-50-56-0c-11-33
15	USERXP	192.200.17.232	00-0c-29-fd-fa-9a

Step 3: Click **Import** to import the users in the equipment. In the **Import Scanning Result** dialog box, select **Create group if no such group on local device**. If the target group for importing the users does not exist, the equipment automatically creates a group during the import. If the **Create group if no such group on local device** option is deselected, the equipment does not create a group during the import, and instead, the users are imported to the root group. Select **Proceed and overwrite existing one** under **If user already exists**. If a user with the same user name already exists in the user list, the attributes of the user are updated. If you select **Skip and not overwrite existing user** and a users with the same user name already exists in the user list, the attributes of the user are not updated, and the user is not imported.

Import Scanning Result

Import scanning result of LAN computers:

☒ Create group if no such group on local device

If user already exists:

☒ Proceed and overwrite existing one

☐ Skip and not overwrite existing user

OK

Cancel

Click **Download to Edit**. The user information is stored in a local CSV file. You can modify the scanning results and user attributes in the CSV file. To import the modified file, click **Import from CSV File**.

Step 4: Click **OK**. The users are imported to the root group.

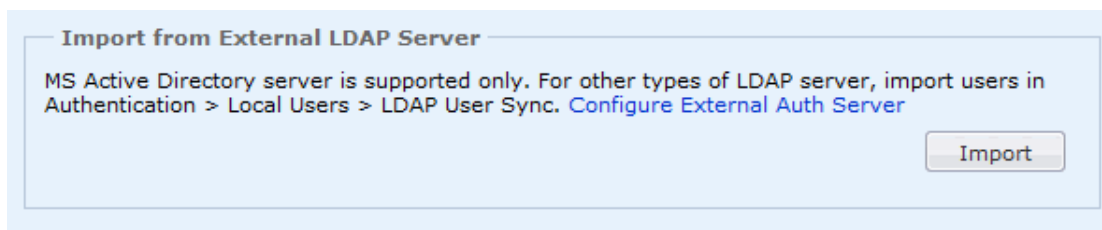


If Username is displayed as unknown, the computer name is not obtained. The computer name is obtained from the console over the NetBIOS protocol. If the computer name is not found during scanning, check whether the NetBIOS protocol is enabled on the target computer, whether multiple IP addresses are configured on the target computer, whether the firewall on the target computer filters the NetBIOS protocol, and whether any equipment on the network filters the NetBIOS protocol.

3.7.1.5.3 Import from External LDAP Server

You can synchronize users on an LDAP server to the equipment. This function is applicable only to the MS Active Directory server. To import users from other types of LDAP servers, choose **Local Users > LDAP User Sync**. For details, see section 3.6.1.5.

Before you import users from an LDAP server, configure the LDAP server. In the navigation area, choose **Authentication > User Authentication > External Auth Server**. For details, see section 3.6.2.3.



1. Controls must be installed for importing users from an LDAP server. Therefore, log in to the console by using the Internet Explorer during the import.
2. When importing users from an LDAP server, the equipment must properly connect to the TCP389 port of the LDAP server, ensuring that user information on the LDAP server can be properly read and obtained.

LDAP Automatic Synchronization

LDAP User Sync is used to synchronize users, organizational structures, and security groups to the equipment and perform automatic synchronization. The equipment automatically synchronizes with the domain server every day at a random time from 00:00 to 06:00.

LDAP User Sync is classified into **Sync by OU** and **Sync by security group (AD domain only)**.

Sync by OU is applicable to all types of LDAP servers. In this synchronization mode, the OUs in the LDAP server are synchronized to the equipment as user groups, and the organizational structures of the OUs are also

synchronized to the equipment in the same form. The users synchronized to the equipment still belong to the corresponding OU groups.

Sync by security group (AD domain only) is only applicable to Microsoft LDAP servers, that is, the AD domain. In this synchronization mode, the security groups in the AD domain server are synchronized to the equipment as user groups. The security group does not have an organizational structure. The equipment synchronizes the security groups at the same level, that is, the synchronized security groups are at the same level.

3.7.1.6.1 Adding a Synchronization Policy

Synchronization policies are used to set parameters related to the synchronization. LDAP synchronization is performed based on the configured synchronization policies.

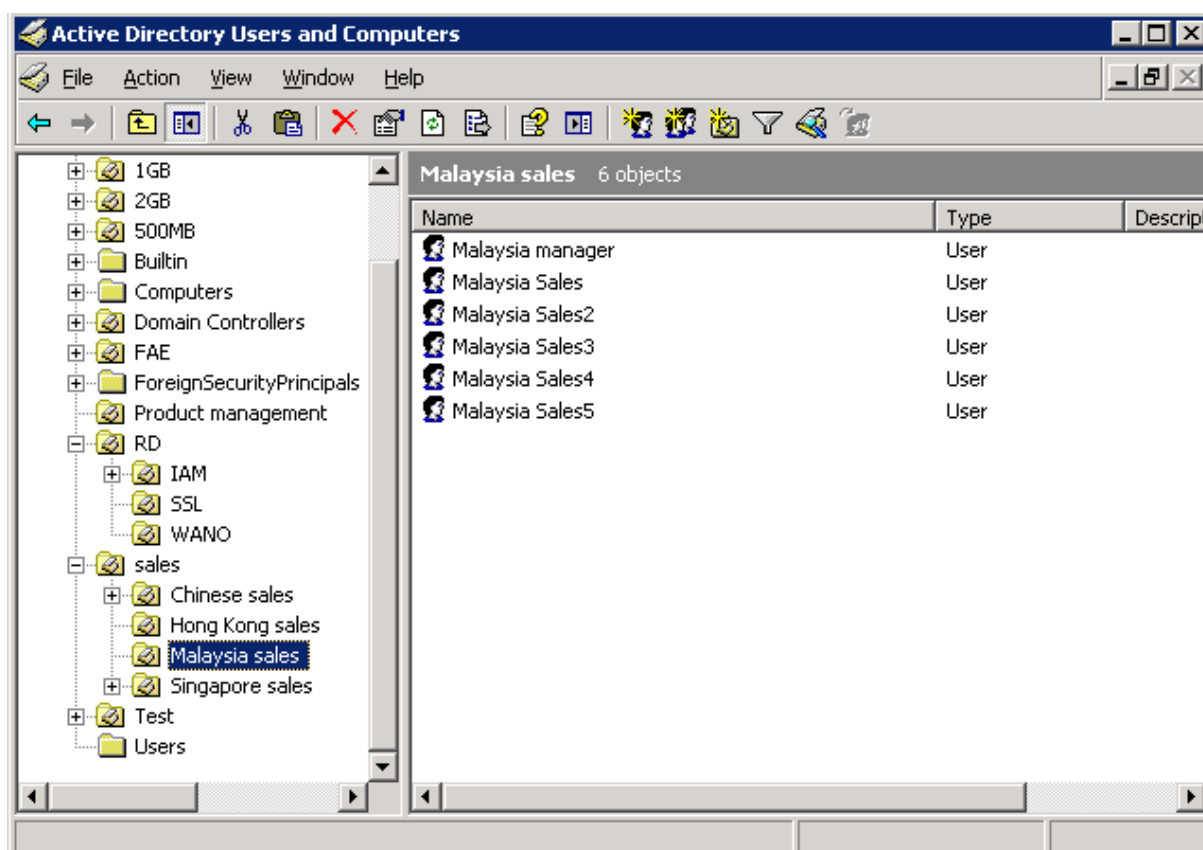
Sync by OU

Sync by OU is applicable to all types of LDAP servers. In this synchronization mode, the OUs in the LDAP server are synchronized to the equipment as user groups, and the organizational structures of the OUs are also synchronized to the equipment in the same form. The users synchronized to the equipment still belong to the corresponding OU groups.

3.7.1.6.1.1 Cases for Sync by OU

OU=engineering department, OU=marketing department, and OU=IT department and the corresponding sub-OUs and users in the LDAP server are required to be synchronized to the equipment.

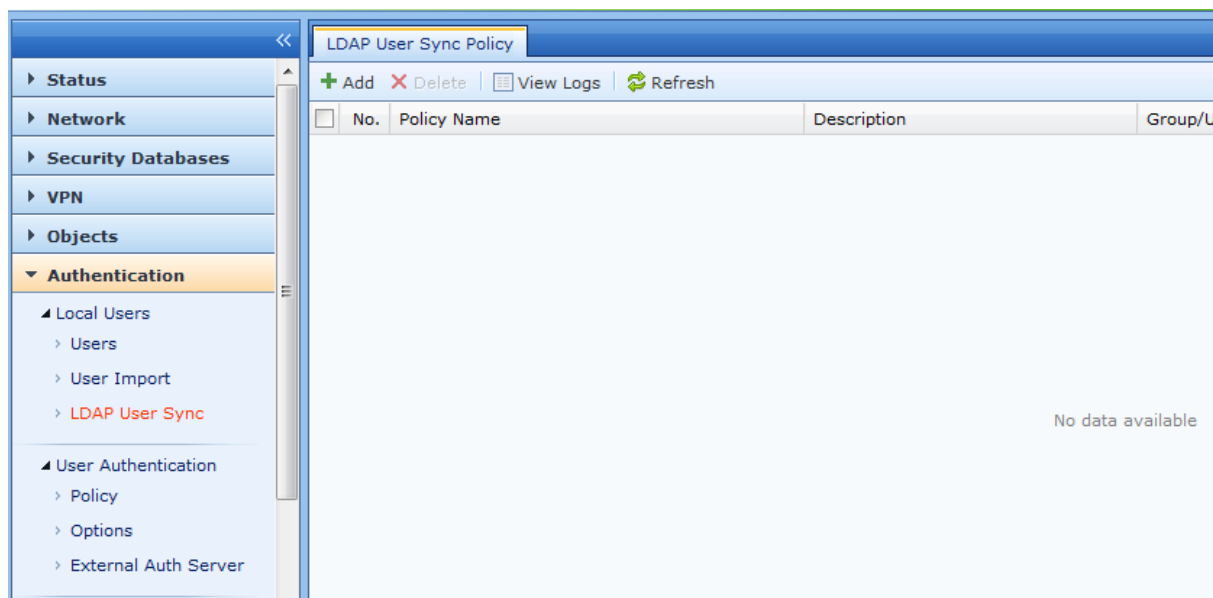
The organizational structure in the LDAP server is as follows:



Procedure:

Step 1: Set the LDAP server to be synchronized. Set the IP address, port number, user name and password for login. In the navigation area, choose **Authentication > User Authentication > External Auth Server**. For details, see section 3.6.2.3.

Step 2: Choose **Authentication > LDAP User Sync**. Click **Add**.



Step 3: In the displayed **Add User Sync Policy** dialog box, set **Policy Name**, **Description**, **Sync Mode**, and **Auto Sync**. Set **Sync Mode** to **Sync by OU** and **Auto Sync** to **Enable (every day)**, so that the synchronization is automatically performed once every day.

The screenshot shows a dialog box titled 'Add User Sync Policy'. It contains four fields: 'Policy Name' with the value 'Sync policy 1', 'Description' with the value 'Sync RD', 'Sync Mode' with a dropdown menu set to 'Sync by OU', and 'Auto Sync' with a dropdown menu set to 'Enable (every day)'. There is an information icon (i) next to the 'Auto Sync' dropdown.

Step 4: Set the related OU information of the LDAP server that needs to be synchronized in **Synchronization Source**.

Add User Sync Policy

Policy Name: Sync Policy 1

Description: Sync RD

Sync Mode: Sync by OU

Auto Sync: Enable (every day)

Synchronization Source

LDAP Server: AD1

Sync with Remote Directory:

Select

OU=RD,DC=sangfor,DC=com

☐ Add user structure based on top-level OU of selected remote directory beneath specified local group
 ☒ Add user structure based on bottom-level OU of selected remote directory beneath specified local group
 ☐ Add user structure based on sub-OU of selected remote directory beneath specified local group

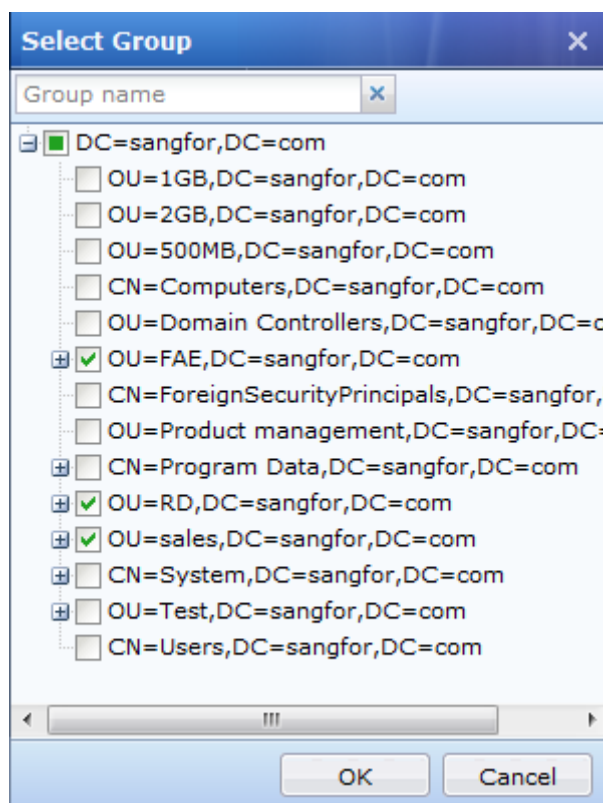
OU Depth: 16

Filter:

OK Cancel

Set the LDAP server to be synchronized in **LDAP Server**. In this step, set the LDAP server to the server configured in step 1.

Specify the OUs in the LDAP server to be synchronized in **Sync with Remote Directory**. Then, click **OK**. In the **Select Group** window, select **OU=FAC**, **OU=RD**, and **OU=sales**. Click **OK**.



If you select **Add user structure based on top-level OU of selected remote directory beneath specified local group**, the root domain names of the LDAP are synchronized as groups and other synchronized OUs are the corresponding subgroups.

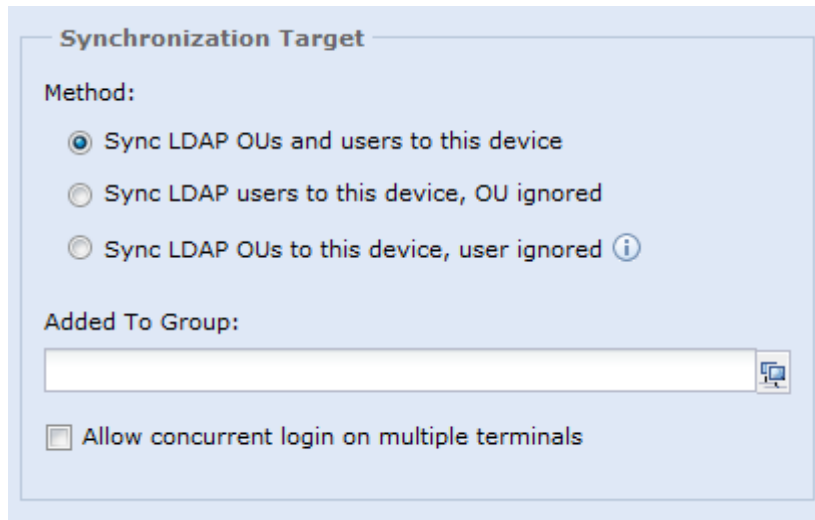
If you select **Add user structure based on bottom-level OU of selected remote directory beneath specified local group**, the synchronization is performed from the selected OUs.

If you select **Add user structure based on sub-OU of selected remote directory beneath specified local group**, the synchronization is performed from the sub-OUs of the selected OUs, and the selected OUs and the direct users of the selected OUs are not synchronized to the equipment.


Set the depth for the imported OUs in **OU Depth**. In this example, set **OU Depth** to **10**, so that 9 levels of the sub-OUs can be synchronized to the equipment as user groups, and OUs lower than level 9 are not synchronized to the equipment as user groups. Users lower than level 9 can still be synchronized to the equipment and belong to level-9 OUs after synchronization.

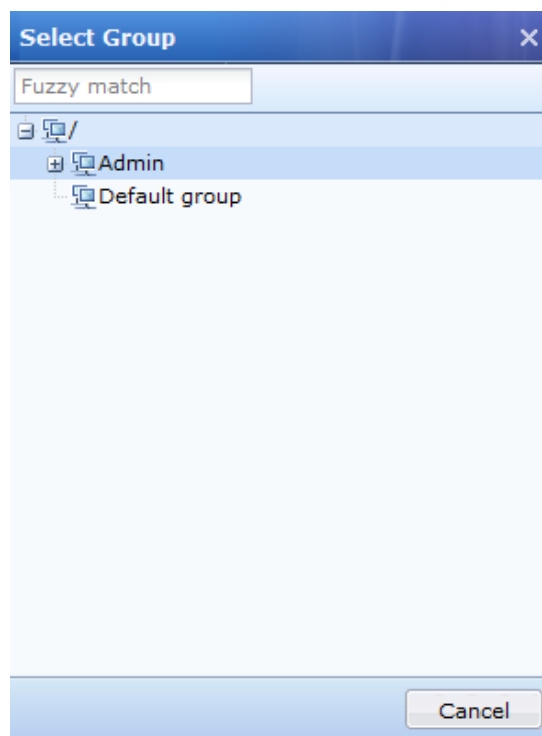
Set the filter parameters for the synchronization in **Filter**.

Step 5: Set the import mode, location where the synchronized OUs and users are stored in the organizational structure, and synchronized user properties in **Synchronization Target**.





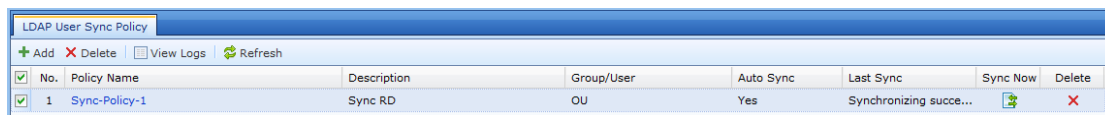
Set whether the OUs and users are synchronization in **Method**. If you select **Sync LDAP OUs and users to this device**, the OUs are synchronized to the equipment as user groups, and meanwhile, the users in the OUs are synchronized to the corresponding user groups of the OUs. If you select **Sync LDAP users to this device, OU ignored**, the users of the OUs are synchronized to the equipment but the OUs are not. If you select **Sync LDAP users to this device, user ignored**, the OUs are synchronized to the equipment as user groups but the users of the OUs are not. In this example, select **Sync LDAP OUs and users to this device**.



Specify an existing group in **Add To Group**, so that the synchronized OUs belong to the sub-groups of the selected OUs. Click . Select the corresponding group in **Select Group**. Then, click **OK**.



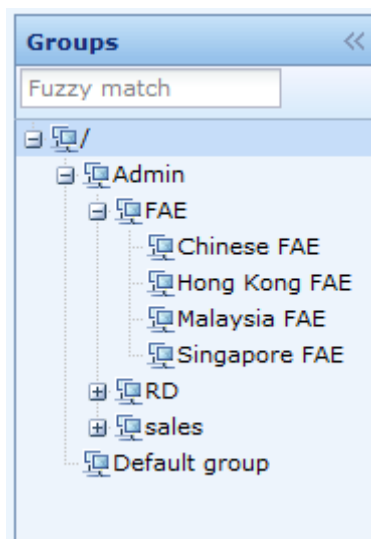
Select **Added To Group**, and **Allow concurrent login on multiple terminals in Synchronization Target**, so that the domain account of the equipment is the public account by default, that is, the same account can be logged in on multiple computers. If this option is not selected, the user is a private account and this account can be logged in on only one computer.

Step 6: Set the synchronization policy. Click **Submit**. You can view the added synchronization policies in **LDAP User Sync Policy** and immediately start the synchronization by clicking . If you do not click , the synchronization is automatically performed once every day.



No.	Policy Name	Description	Group/User	Auto Sync	Last Sync	Sync Now	Delete
1	Sync-Policy-1	Sync RD	OU	Yes	Synchronizing succe...		

Step 7: Choose **User Management > Groups** to check the organizational structure. As shown in the following figure, the imported OUs and users are consistent with those in the LDAP server.



If the names of the user groups or users in the equipment are the same as those of the user groups and users in the OUs to be synchronized, the OUs and users in the LDAP cannot be synchronized to the equipment.

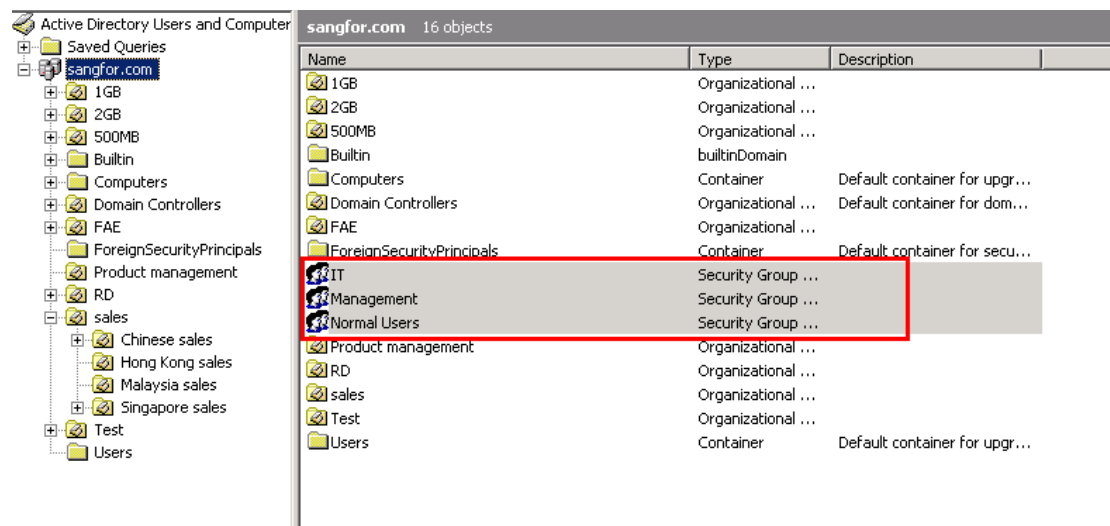
Sync by security group (AD domain only)

This synchronization mode is only applicable to the MS Active Directory server, that is, the AD domain. In this synchronization mode, the security groups in the AD domain server are synchronized to the equipment as user groups. The security group does not have an organizational structure. The equipment synchronizes the security groups at the same level, that is, the synchronized security groups are at the same level.

3.7.1.6.1.1 Cases for Sync by security group (AD domain only)

CN=IT, CN=Management, and CN=Normal Users in the LDAP server and the users in the corresponding security groups are required to be synchronized to the equipment.

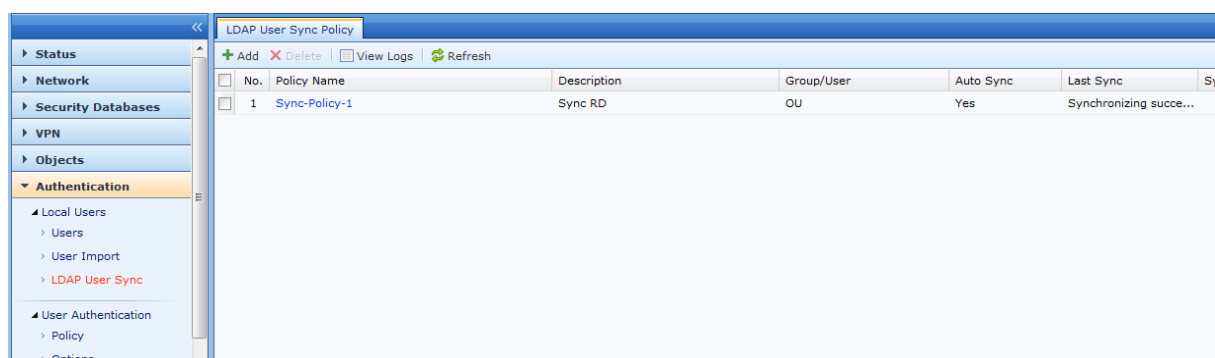
The security groups in the LDAP server are as follows:



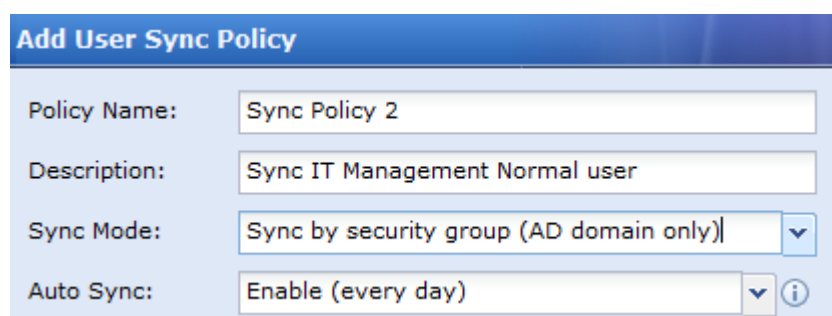
Procedure:

Step 1: Set the LDAP server to be synchronized. Set the IP address, port number, user name and password for login. In the navigation area, choose **Authentication > User Authentication > External Auth Server**. For details, see section 3.6.2.3.

Step 2: Choose **Authentication > LDAP User Sync**. Click **Add**.



Step 3: In the displayed **Add User Sync Policy** dialog box, set **Policy Name**, **Description**, **Sync Mode**, and **Auto Sync**. Set **Sync Mode** to **Sync by security group (AD domain only)** and **Auto Sync** to **Enable (every day)**, so that the synchronization is automatically performed once every day.




Step 4: Set the related security group information of the LDAP server that needs to be synchronized in **Synchronization Source**.

Add User Sync Policy




Synchronization Source


LDAP Server:


Sync with Remote Directory:

 Select

CN=IT,DC=sangfor,DC=com
 CN=Management,DC=sangfor,DC=com
 CN=Normal Users,DC=sangfor,DC=com


☐ Add user structure based on top-level OU of selected remote directory beneath specified local group 
☒ Add user structure based on bottom-level OU of selected remote directory beneath specified local group 
☐ Add user structure based on sub-OU of selected remote directory beneath specified local group 

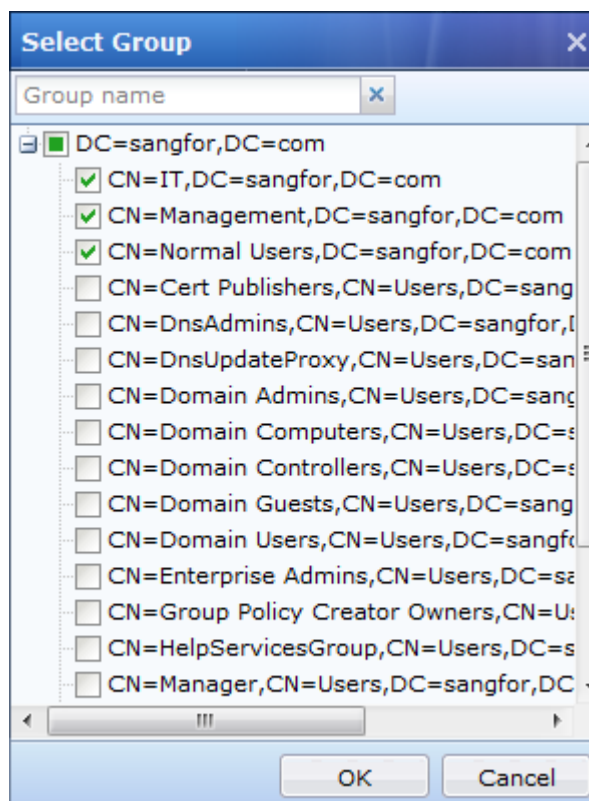
OU Depth: 

Filter: 

LDAP Server is used to set the LDAP server to be synchronized. In this step, set the LDAP server to the server configured in step 1.

Specify the security groups in the LDAP server to be synchronized in **Sync with Remote Directory**. Click

 **Select**. In **Select Group**, select **CN=IT**, **CN=Management**, and **CN=Normal Users**. Click **OK**.



If you select **Add user structure based on top-level OU of selected remote directory beneath specified local group**, the root domain names of the LDAP are synchronized as groups and other synchronized OUs are the corresponding subgroups.

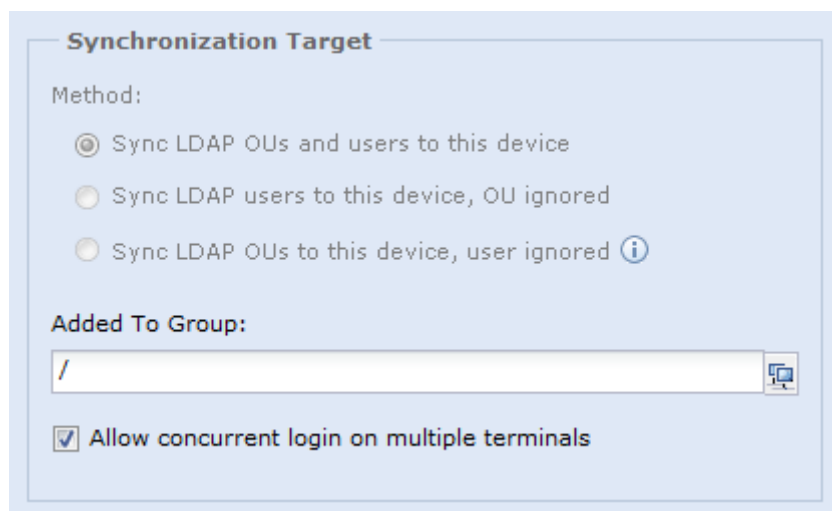
If you select **Add user structure based on bottom-level OU of selected remote directory beneath specified local group**, the synchronization is performed from the selected OUs.

If you select **Add user structure based on sub-OU of selected remote directory beneath specified local group**, the synchronization is performed from the sub-OUs of the selected OUs, and the selected OUs and the direct users of the selected OUs are not synchronized to the equipment.


OU Depth does not need to be configured for security group synchronization.

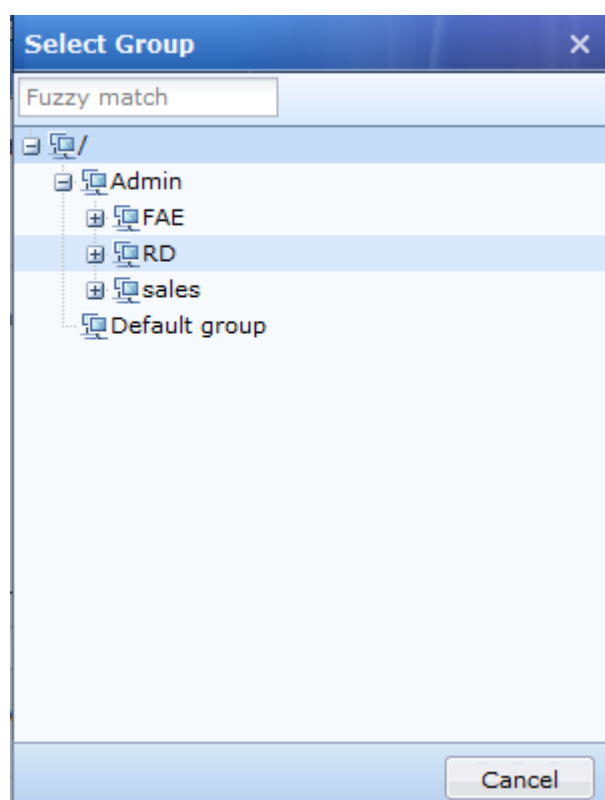
Set the filter parameters for the synchronization in **Filter**.

Step 5: Set the import mode, location where the synchronized security groups and users are stored in the organizational structure, and synchronized user properties in **Synchronization Target**.





Method does not need to be configured. By default, the security groups and users are synchronized to the equipment.

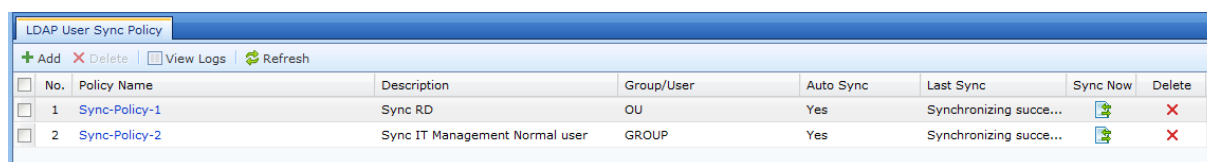
Specify an existing group in **Add To Group**, so that the synchronized security groups belong to the sub-groups of the selected OUs. Click . Select the corresponding group in **Select Group**. Then, click **OK**.







Select **Added To Group**, and **Allow concurrent login on multiple terminals** in **Synchronization Target**, so that the domain account of the equipment is the public account by default, that is, the same account can be logged in on multiple computers. If this option is not selected, the user is a private account and this account can be logged in on only one computer.

Step 6: Set the synchronization policy. Click **Submit**. You can view the added synchronization policies in **LDAP**

User **Sync Policy** and immediately start the synchronization by clicking . If you do not click , the synchronization is automatically performed once every day.



No.	Policy Name	Description	Group/User	Auto Sync	Last Sync	Sync Now	Delete
1	Sync-Policy-1	Sync RD	OU	Yes	Synchronizing succe...		
2	Sync-Policy-2	Sync IT Management Normal user	GROUP	Yes	Synchronizing succe...		

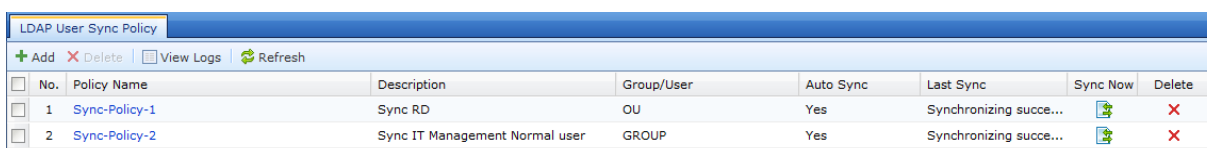
Step 7: Choose **User Management > Groups** to check the organizational structure. As shown in the figure below, the imported security groups and users are consistent with those in the LDAP server.







If the names of the user groups or users on the equipment are the same as those of the user groups and users in the security groups to be synchronized, the security groups and users in the LDAP cannot be synchronized to the equipment.

3.7.1.6.2 Deleting a Synchronization Policy

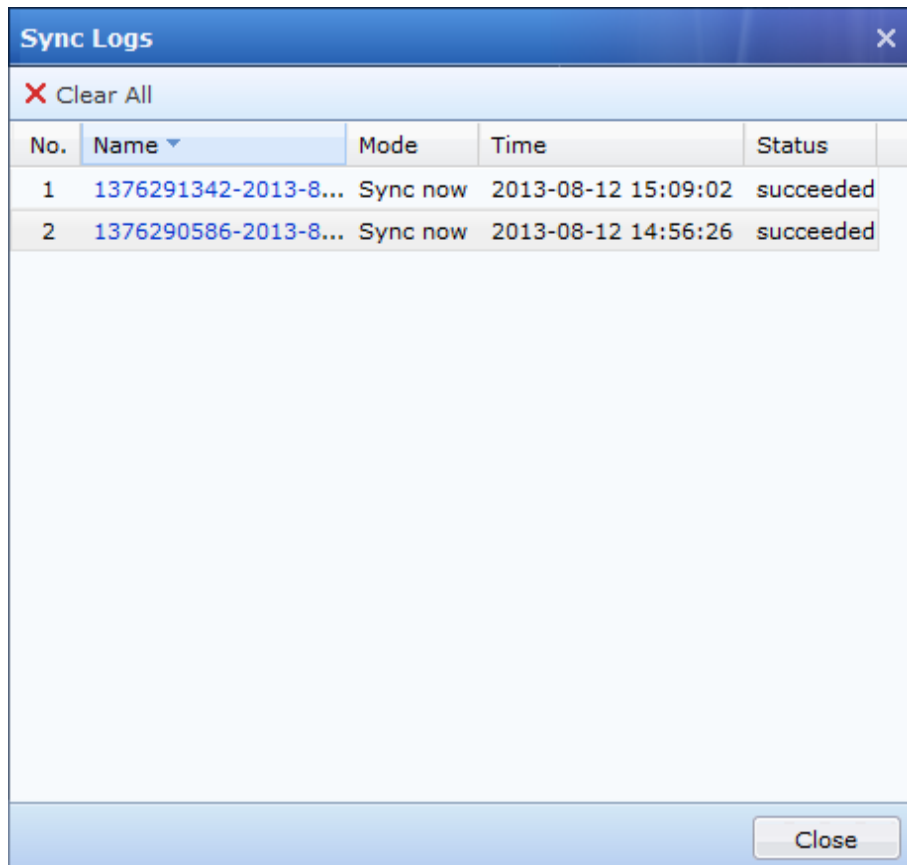
To delete a useless synchronization policy, select the synchronization policy on the **LDAP User Sync Policy** page, and click Delete. Deleting a synchronization policy does not affect the groups and users that have been synchronized to the equipment.



No.	Policy Name	Description	Group/User	Auto Sync	Last Sync	Sync Now	Delete
1	Sync-Policy-1	Sync RD	OU	Yes	Synchronizing succe...		
2	Sync-Policy-2	Sync IT Management Normal user	GROUP	Yes	Synchronizing succe...		

3.7.1.6.3 Checking Synchronization Logs

The NGAF generates a synchronization log each time it executes an LDAP synchronization. You can view the logs to learn about the synchronization process and result. Click **View Logs**. On the displayed **Sync Logs** screen, select the required log item, download the log, and check the content.



User Authentication

The **User Authentication** menu is used for user authentication settings, with submenus of **Policy**, **Options**, and **External Auth Server**. If user authentication is not enabled on the NGAF, Intranet users can still access the Internet. To prevent Intranet users from accessing the Internet, you can define IP addresses in objects to protect the PCs on the Intranet. In this case, users and logs are listed by IP addresses.

Authentication Policies

3.7.2.1.1 Overview

If user authentication is enabled on the NGAF, all computers in the authentication zone must be authenticated and identified before accessing the Internet. The authentication policy defines how the computers with specific IP addresses or MAC addresses, or in a specific network segment are authenticated. You can set an authentication policy to define the authentication mode of Intranet users and the policies for adding new users.

The NGAF verifies authentication policies from top to bottom one by one. You can adjust the order of the authentication policies to change the priority by the button of the scroll bar on the screen. The authentication policies allow you to set different authentication modes for computers in different network segments.

Authentication modes:

The NGAF supports the following authentication modes:

1. No authentication;
2. Password authentication (including local password authentication and external server authentication);
3. Single sign-on (SSO) authentication. The authentication modes are set under the sub-menu **Policy**. For SSO authentication, configuration must be also done under the sub-menu **Option**.

The authentication modes available in Policy are None/SSO, SSO, Local or external password authentication, and SSO only.



All three options include SSO authentication. If SSO authentication is configured in Authentication Option, the user name is used in priority for Internet access after the user name of the computer is identified using the SSO function.

1. None/SSO

If this option is selected and SSO authentication is configured in **Authentication Option**, the user name is used in priority for Internet access after the user name of the computer is identified using the SSO function.

If this option is selected and SSO authentication is not configured, the NGAF identifies users based on the source IP addresses, source MAC addresses, and computer names of the data packet. In this authentication mode, the authentication dialog box requesting the user name and password does not pop up on the Web browser before the user accesses the Internet. That is, the user does not feel the existence of the NGAF.

How to create a user account not requiring authentication?

In the **Authentication Policy** screen, select **None/SSO** for **Authentication**. Apply bidirectional bindings between the user and the IP/MAC address while creating the user account. In this case, a one-to-one relationship is defined between the IP/MAC address and the user, and the user can be identified by the IP/MAC address. (The IP/MAC address segment specified in **Authentication Policy** must contain the bound IP/MAC address).

Or, In the **Authentication Policy** screen, select **None/SSO** for **Authentication**. Use the IP address, MAC address, or computer name as the user name. The Intranet user is authenticated based on the IP address, MAC address, or computer name that matches the user name.

2. SSO, Local or external password authentication

This authentication mode is enabled when the user authentication function is enabled on the NGAF and **SSO, Local or external password authentication** is selected.

If the SSO authentication is not configured or is not successful, the authentication process for Internet access is as follows:

Step 1 A dialog box requesting the user name and password is opened on the Web browser. Assume the input user name is **test** and the password is **password**.

Step 2 The NGAF checks for user test among local users. If the user exists and has the local password (that is, **Local password** is selected in **User Attributes**), the NGAF checks whether the local password is **password**. If the password is correct, the authentication succeeds; if not, the authentication fails.

Step 3 If user test does not exist as a local user, or user test exists as a local user with the local password not

being configured, the NGAF checks for the user name and password on the external authentication server. If the user name and password are correct, the authentication succeeds; if not, the authentication fails.

In conclusion, local authentication is executed in prior to external authentication.

3. SSO only

If this option is selected, computers within the address range specified in **Policy** can access the Internet only after successful SSO authentication.

Configuration:

Step 1 Set the authentication policy for the specified network segment as **SSO only**.

Step 2 In **Authentication Option**, select **SSO only**. For a domain SSO, set the domain server accordingly. (See section 3.6.2.2.1).

You can set exceptional users for SSO authentication. In this case, those users only have to input the user name and password for authentication before accessing the Internet.

Handling new users:

New users refer to users that do not exist in the NGAF. For these users, the NGAF matches their IP or MAC addresses to the authentication policy, and checks whether to add these users based on the settings of **New User Option** in **Authentication Policy**.

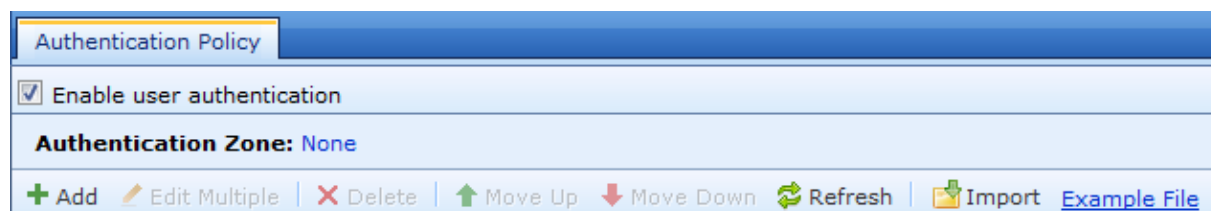
The users successfully authenticated are added automatically, including the following: 1. Users authenticated based on the following configuration: **None/SSO** is enabled in **Authentication**, and **Take IP as username**, **Take MAC as username**, or **Take host name as username** is selected in **New User Option**. 2. SSO users. 3. Users authenticated with external passwords.

You can choose one of the following options to handle new users: **Added to specific local groups**, **Added as casual account (not to any local group)**, and **No authentication for new users**.

3.7.2.1.2 Selecting Authentication Zone

Before setting an authentication policy, select zones for the authentication settings. For details about how to set up an authentication zone, see section 3.2.1.4.

Step 1 Select **Enable user authentication**.



Step 2 Select the zones where the authentication policy is applied.

Select Authentication Zone		X
<input type="checkbox"/>	Name	Forward Mode
<input type="checkbox"/>	InternalZone	Bridge(layer 2)
<input type="checkbox"/>	InternetZone	Bridge(layer 2)
<input type="checkbox"/>	ExternalZone	Route(layer 3)
<input type="checkbox"/>	InternalZonetest	Route(layer 3)
<input type="checkbox"/>	Trusted-UKM	Route(layer 3)
<input type="checkbox"/>	External-UKM	Route(layer 3)

Click **OK**. The authentication zones are set.



You can choose the zone where the intranet port locates as the authentication zone. The zones can also be defined by intranet interfaces or Ethernet interfaces. For example, interface ETH2 is a WAN interface while ETH1 is a non-WAN interface. That is, interface ETH2 can be defined as an Ethernet zone and ETH1 as an intranet zone.

3.7.2.1.3 Adding an Authentication Policy

3.7.2.1.3.1 Configuration Example 1

Set a third-party password authentication policy based on LDAP servers for the network segment 192.168.1.0/255.255.255.0 of the IT department. The new users are automatically added to the IT group, with user names and IP addresses bound bidirectionally. That is, the user name must in one-to-one correspondence with the IP address. Other network segments on the intranet do not require authentication. The IP address is taken as the user name. The new users are automatically added to the Default group. (In this example, the LDAP server is taken as an external server. The steps for setting up external authentication for other types of external servers are similar.)

Step 1 Set the LDAP external authentication server in **External Auth Server**. (For details, see section 4.6.2.3.)

Step 2 Choose **User Authentication > Policy**. Click **Add**. The **Authentication Policy** screen appears.

Specify the policy name in **Policy Name**, which is mandatory.

In **Description**, enter the description of the policy. The parameter is optional.

In **IP/MAC Range**, enter the IP addresses, IP address range, or MAC addresses. If a user for authentication does not match the range specified here, the NGAF checks the IP or MAC address of the data packet and applies the authentication policy accordingly. In this example, set **IP/MAC Range** to **192.168.1.0/255.255.255.0**.

Authentication Policy

Name: Subnet 1

Description:

IP/MAC Range: i
192.168.1.0/255.255.255.0

Step 3 Choose **Policy**. Select an authentication mode for **Authentication**.

The authentication modes available in **Authentication** are **Non/SSO**, **SSO**, **Local or external password authentication**, and **SSO only**. (For details about the authentication modes, see section 3.6.2.1.1.)

In this example, choose **SSO, Local or external password authentication**.

Authentication

☐ None/SSO

- ☒ Take IP as username
- ☐ Take MAC as username
- ☐ Take host name as username

If SSO is configured, the detected username is preferable

☒ SSO, Local or external password authentication i

The browser will be redirected to an authentication page when user attempts to access the Internet, on which user credential are required. [Configure External Auth Server](#)

☐ SSO only i

Excluded Users: Login name (comma-separated)

Step 4 Choose **Policy**, and set **New User Option**.

New User Option (for users outside local device)

☒ **Added to specified local group**

Select Group:

☐ **Not applied to new users authenticated against external LDAP server (for they can be synchronized to a corresponding group automatically).**
User Sync Policy

Other User Attributes:

Concurrent Login:

☒ Allow concurrent login on multiple terminals

☐ Only allow login on one terminal

☐ **Bind IP/MAC:** [Binding Mode](#)

☒ Bind the IP on initial logon

☐ Bind the MAC on initial logon

☐ Bind the IP and MAC on initial logon

☐ **Added as casual account (not to any local group), with same privilege as**

User Group:

☐ **No authentication for new users**

If **Added to specified local group** is selected, the new users are added automatically to the user list in the NGAF. The **Select Group** parameter specifies which user group new users are added to. In this example, the new users authenticated by a third party are added to the IT group. Therefore, choose **IT** for **Select Group**.

If **Not applied to new users authenticated against external LDAP server** is selected, users authenticated against a third-party LDAP server or by SSO are synchronized to the NGAF based on the configured LDAP synchronization policy if there's any, and are added to the corresponding group, prior to the configuration of **Select Group**.

Under **Other User Attributes**, the **Concurrent Login** and **Bind IP/MAC** parameters can be specified.

The options for **Concurrent Login** are **Allow concurrent login on multiple terminals** and **Only allow login on one terminal**. The configuration takes effect only for authenticated users.

The binding mode for IP/MAC binding can be one-way or bidirectional.

One-way binding: The user can be authenticated using only a dedicated address, and other users can also use the same address for authentication.

Bidirectional binding: The user can be authenticated using only a dedicated address, and other users cannot use the same address for authentication.

In this example, select **Bidirectional binding**, and **Bind the IP on initial logon**.

If **Added as casual account** is selected, the new users are not added to the user list and access the Internet with

only temporary user privileges. If **User Group** under this option is specified, the new users access the Internet with privileges of the specified user group.

If **No authentication for new users** is selected, the new users are not added to the user list and do not pass the authentication. In this case, the new users are not allowed to access the Internet and have only the privileges specified for unauthenticated users under **User Authentication > Options > Other Auth Options**.

Step 5 Set the parameters as follows if manual user adding is necessary: Set **Name** to the user name on the external authentication server. Do not select **Local password**. If **Local password** is selected, the user is authenticated locally rather than being authenticated against the external server. Select **Bind IP/MAC** and set the IP address to be bound.

Add User

☒ Enable user

Name:

Description:

Display Name:

Added To Group:

User Attributes

☐ Local password ⓘ

Password:

Confirm:

☒ Bind IP/MAC: [Binding Mode](#)

☒ IP Address ⓘ ☐ MAC Address ⓘ ☐ IP and MAC ⓘ

One entry per row. Annotation is separated by #. Example: #200.200.0.1

☐ Allow concurrent login on multiple terminals ⓘ

☐ Show Logout page if user passes password based authentication

Expiry Date: ☒ Never expire ☐ Date

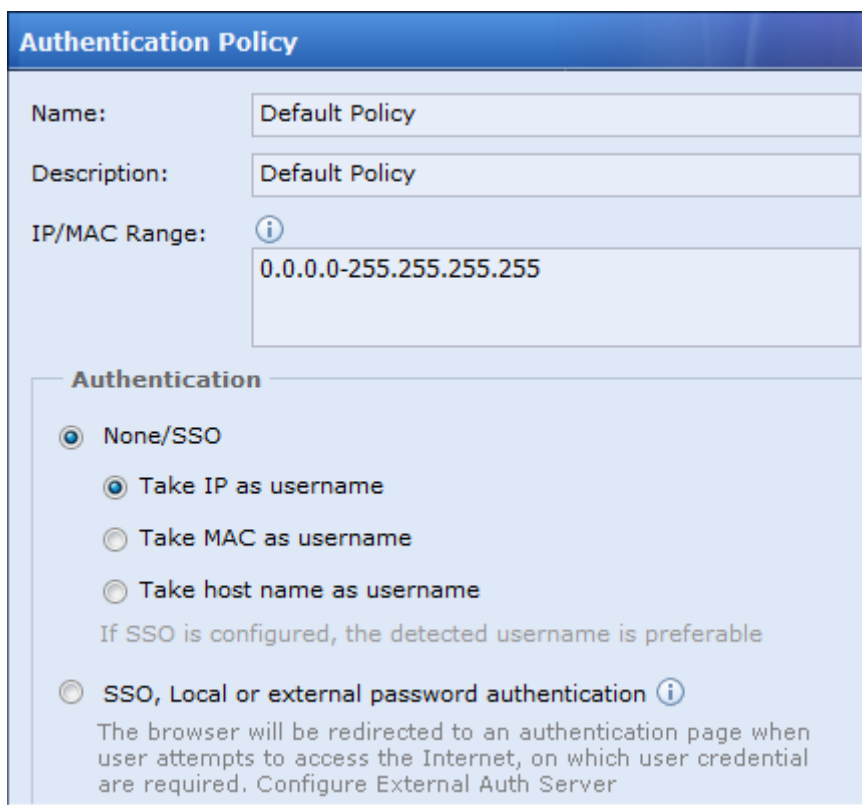
Step 6 Set the authentication policy for users on other network segments as follows:

Requirement: Other network segments on the intranet do not require authentication. The IP address is taken as the

user name. The new users are automatically added to the Default group.

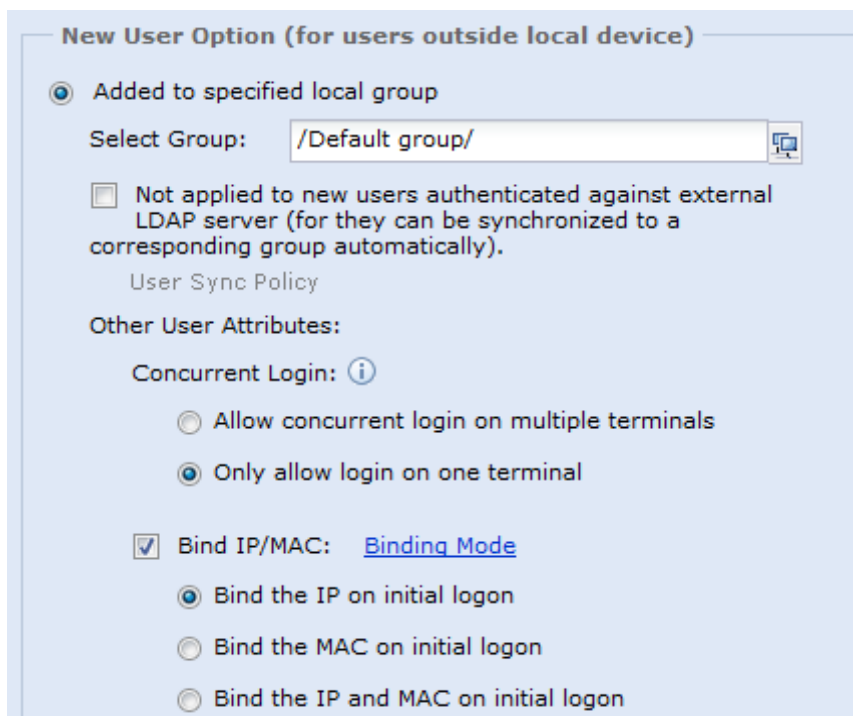
Choose **Policy** and edit the Default Policy.

Select **None/SSO** and **Take IP as username** under **Authentication**.



The screenshot shows the 'Authentication Policy' configuration window. The 'Name' and 'Description' fields are both set to 'Default Policy'. The 'IP/MAC Range' is set to '0.0.0.0-255.255.255.255'. Under the 'Authentication' section, the 'None/SSO' radio button is selected. Below it, the 'Take IP as username' radio button is also selected. Other options include 'Take MAC as username' and 'Take host name as username'. A note states: 'If SSO is configured, the detected username is preferable'. At the bottom, there is an option for 'SSO, Local or external password authentication' with an information icon and a descriptive text: 'The browser will be redirected to an authentication page when user attempts to access the Internet, on which user credential are required. Configure External Auth Server'.

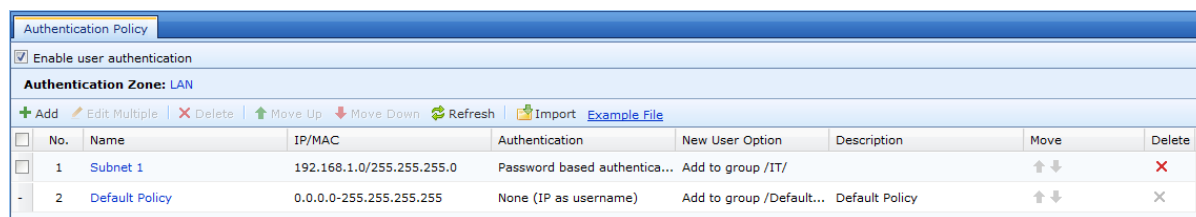
In **New User Option**, select **Added to specified local group** and select **Default group**.



The screenshot shows the 'New User Option (for users outside local device)' configuration window. The 'Added to specified local group' radio button is selected. The 'Select Group' dropdown menu is set to '/Default group/'. There is a checkbox for 'Not applied to new users authenticated against external LDAP server (for they can be synchronized to a corresponding group automatically)' with a note 'User Sync Policy'. Under 'Other User Attributes', the 'Concurrent Login' section has two options: 'Allow concurrent login on multiple terminals' and 'Only allow login on one terminal', with the latter being selected. The 'Bind IP/MAC' checkbox is checked, and the 'Binding Mode' section has three options: 'Bind the IP on initial logon' (selected), 'Bind the MAC on initial logon', and 'Bind the IP and MAC on initial logon'.

The NGAF verifies authentication policies from top to bottom one by one. For the two authentication policies

configured in this example, the order should be the same as the order in the following figure:



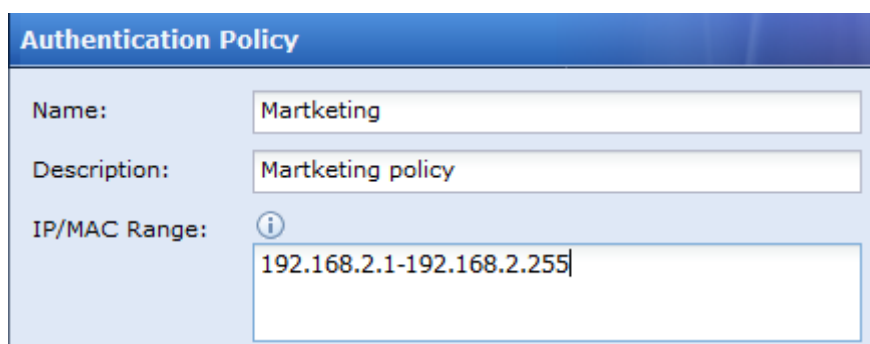
No.	Name	IP/MAC	Authentication	New User Option	Description	Move	Delete
1	Subnet 1	192.168.1.0/255.255.255.0	Password based authentica...	Add to group /IT/		↑ ↓	×
2	Default Policy	0.0.0.0-255.255.255.255	None (IP as username)	Add to group /Default...	Default Policy	↑ ↓	×

3.7.2.1.3.2 Configuration Example 2

The IP address range on the Intranet is *192.168.2.1 to 192.168.2.255*. The computers within the IP address range are added automatically as new users. The authentication mode is no authentication and the computer name is taken as the user name. The binding mode is bidirectional binding by MAC address. New users are added to the Marketing group.

Step 1 Choose **User Authentication > Options > Obtain MAC By SNMP**, and set the options on the **Obtain MAC By SNMP** screen. (For details, see section 4.6.2.2.4.)

Step 2 On the **Authentication Policy** screen, click Add. The **Authentication Policy** screen is displayed. Enter the name and description of the policy.



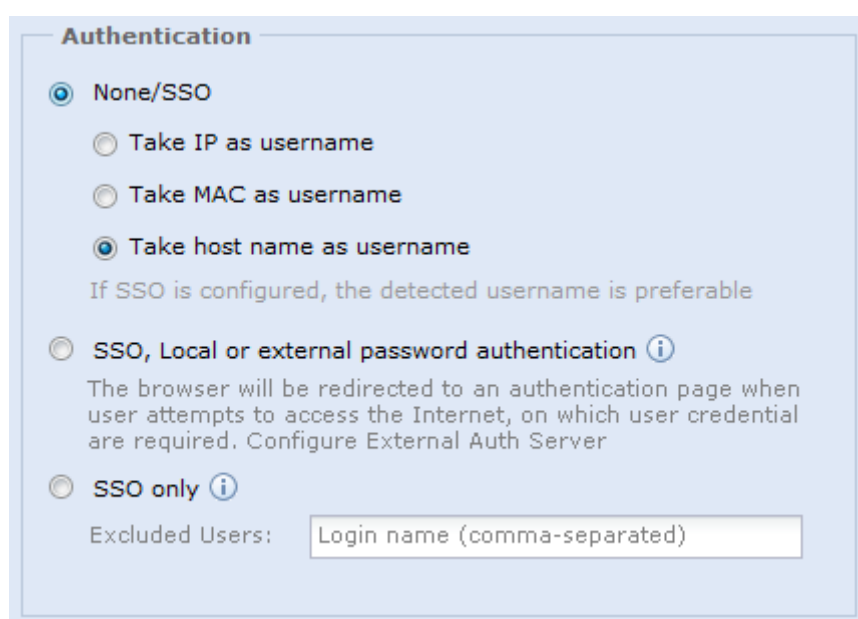
Authentication Policy

Name:

Description:

IP/MAC Range:

Step 3 Select **None/SSO** and **Take host name as username** under **Authentication**.



Authentication

☒ None/SSO

☐ Take IP as username

☐ Take MAC as username

☒ Take host name as username

If SSO is configured, the detected username is preferable

☐ SSO, Local or external password authentication ⓘ

The browser will be redirected to an authentication page when user attempts to access the Internet, on which user credential are required. Configure External Auth Server

☐ SSO only ⓘ

Excluded Users:

Step 4 In **New User Option**, select **Added to specified local group** and select **Marketing**.

Select **Bind IP/MAC** and **Bind the MAC on initial logon**. In this example, as the MAC address is obtained from the switch over the SNMP, you need to set the MAC address obtaining option under **User Authentication > Options > Obtain MAC By SNMP**.

New User Option (for users outside local device)

☒ Added to specified local group

Select Group:

☐ Not applied to new users authenticated against external LDAP server (for they can be synchronized to a corresponding group automatically).

User Sync Policy

Other User Attributes:

Concurrent Login:

☒ Allow concurrent login on multiple terminals

☐ Only allow login on one terminal

☒ Bind IP/MAC: [Binding Mode](#)

☐ Bind the IP on initial logon

☒ Bind the MAC on initial logon

☐ Bind the IP and MAC on initial logon

☐ Added as casual account (not to any local group), with same privilege as

User Group:

☐ No authentication for new users

Step 5 Click Submit. The policy is successfully edited.

Authentication Policy								
<input checked="" type="checkbox"/> Enable user authentication								
Authentication Zone: LAN								
+ Add Edit Multiple Delete Move Up Move Down Refresh Import Example File								
<input type="checkbox"/>	No.	Name	IP/MAC	Authentication	New User Option	Description	Move	Delete
<input type="checkbox"/>	1	Marketing	192.168.2.1-192.168.2.255	None(host name as userna...	Add to group /Marketi...	Marketing policy		
<input type="checkbox"/>	2	Subnet 1	192.168.1.0/255.255.255.0	Password based authentica...	Add to group /IT/			
<input type="checkbox"/>	3	Default Policy	0.0.0.0-255.255.255.255	None (IP as username)	Add to group /Default...	Default Policy		



- The NGAF obtains host names of the Internet accessing computers over the NETBIOS protocol. The host name may not be obtained successfully. In this case, check whether the NETBIOS protocol is enabled on the computer, whether the computer is configured with multiple IP addresses, whether the

firewall on the computer filters out the NETBIOS protocol, and whether a device on the network path is deployed with NETBIOS protocol filtering. If the host name cannot be obtained, the NGAF takes the computer as a new user with the name of Unknown Computer. The computer can be queried only in the online user list and is not added to the specified local user group.

- If one or multiple L3 switches are deployed between the computer trying for Internet access and the equipment room, the MAC address of the computer is changed. In this case, the NGAF cannot obtain the actual MAC address of the computer. The problem can be solved in the following way:

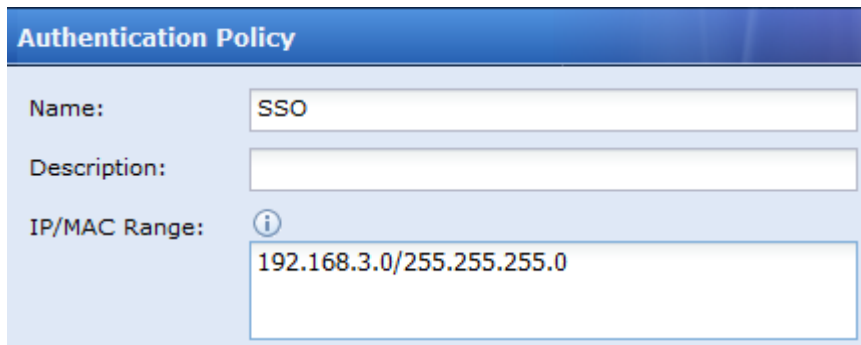
Obtain the ARP list of the L3 switch which is most close to the computer (that is, the destination gateway of the data packet sent by the computer for Internet access). Check the original MAC address of the specified IP address from the ARP list.

3.7.2.1.3.3 Configuration Example 3

The computers on the network segment 192.168.3.0/255.255.255.0 are authenticated using the AD domain SSO. That is, only when the user in the AD domain is authenticated successfully against AD domain and the NGAF, the user can be synchronized to the NGAF. If the SSO of the computer on the network segment fails, the IP address is taken as the user name and no authentication is required. The user is added to the Default group automatically.

Step 1 Set the LDAP external authentication server in **External Auth Server** and the LDAP user synchronization configuration in **LDAP User Sync**. (For details, see sections 4.6.2.3 and 4.6.1.5.)

Step 2 On the **Authentication Policy** screen, click **Add**. The **Authentication Policy** screen is displayed. Enter the name and description of the policy.



Step 3 Select **None/SSO** and **Take IP as username** under **Authentication**.

Authentication

☒ **None/SSO**

☒ Take IP as username

☐ Take MAC as username

☐ Take host name as username

If SSO is configured, the detected username is preferable

☐ **SSO, Local or external password authentication** ⓘ

The browser will be redirected to an authentication page when user attempts to access the Internet, on which user credential are required. Configure External Auth Server

☐ **SSO only** ⓘ

Excluded Users:

Step 4 In **New User Option**, select **Added to specified local group** and select **Marketing**. The users not implementing SSO are added to the Default group and the Internet access policy of the default group is applied to these users.

Select **Not applied to new users authenticated against external LDAP server**. The users using domain SSO are added to the user group specified in the synchronization rule.

Do not select **Bind IP/MAC**. Because if users not implementing SSO are added as new users and are applied with IP/MAC bidirectional binding, the IP/MAC address can only be used by that user and can no longer be used in SSO authentication. You can set one-way binding.

New User Option (for users outside local device)

☒ Added to specified local group

Select Group:

☐ Not applied to new users authenticated against external LDAP server (for they can be synchronized to a corresponding group automatically).

User Sync Policy

Other User Attributes:

Concurrent Login:

☒ Allow concurrent login on multiple terminals

☐ Only allow login on one terminal

☐ Bind IP/MAC: [Binding Mode](#)

☒ Bind the IP on initial logon

☐ Bind the MAC on initial logon

☐ Bind the IP and MAC on initial logon

☐ Added as casual account (not to any local group), with same privilege as

User Group:

☐ No authentication for new users

Step 5 Click Submit. The policy is successfully edited.

Authentication Policy								
<input checked="" type="checkbox"/> Enable user authentication								
Authentication Zone: LAN								
+ Add Edit Multiple Delete Move Up Move Down Refresh Import Example File								
<input type="checkbox"/>	No.	Name	IP/MAC	Authentication	New User Option	Description	Move	Delete
<input type="checkbox"/>	1	SSO	192.168.3.0/255.255.255.0	None (IP as username)	Add to group /		↑ ↓	×
<input type="checkbox"/>	2	Marketing	192.168.2.1-192.168.2.255	None(host name as userna...	Add to group /Marketi...	Marketing policy	↑ ↓	×
<input type="checkbox"/>	3	Subnet 1	192.168.1.0/255.255.255.0	Password based authentica...	Add to group /IT/		↑ ↓	×
<input type="checkbox"/>	4	Default Policy	0.0.0.0-255.255.255.255	None (IP as username)	Add to group /Default...	Default Policy	↑ ↓	×

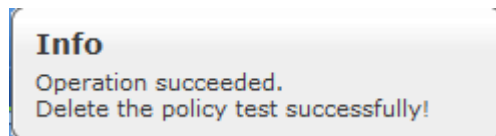
3.7.2.1.4 Deleting Authentication Policies

Take the new user authentication policy test as an example.

Step 1 Select policy test.

Authentication Policy								
<input checked="" type="checkbox"/> Enable user authentication								
Authentication Zone: LAN								
+ Add Edit Multiple Delete Move Up Move Down Refresh Import Example File								
<input type="checkbox"/>	No.	Name	IP/MAC	Authentication	New User Option	Description	Move	Delete
<input checked="" type="checkbox"/>	1	test	192.168.4.0/255.255.255.0	None (IP as username)	Add to group /		↑ ↓	×
<input type="checkbox"/>	2	SSO	192.168.3.0/255.255.255.0	None (IP as username)	Add to group /		↑ ↓	×
<input type="checkbox"/>	3	Marketing	192.168.2.1-192.168.2.255	None(host name as userna...	Add to group /Marketi...	Marketing policy	↑ ↓	×
<input type="checkbox"/>	4	Subnet 1	192.168.1.0/255.255.255.0	Password based authentica...	Add to group /IT/		↑ ↓	×
-	5	Default Policy	0.0.0.0-255.255.255.255	None (IP as username)	Add to group /Default...	Default Policy	↑ ↓	×

Step 2 Click Delete and confirm the deletion. The policy is deleted successfully.



3.7.2.1.5 Editing Authentication Policies in Batches

You can edit the attributes of multiple authentication policies in batches, except for names and descriptions.

In this example, change the authentication mode to no authentication for users in the Marketing group on network segment 1, and change the new user authentication option to taking the host name as the user name.

Step 1 Select authentication policies **Marketing** and **Subnet 1**.

Authentication Policy								
<input checked="" type="checkbox"/> Enable user authentication								
Authentication Zone: LAN								
+ Add Edit Multiple Delete Move Up Move Down Refresh Import Example File								
<input type="checkbox"/>	No.	Name	IP/MAC	Authentication	New User Option	Description	Move	Delete
<input type="checkbox"/>	1	SSO	192.168.3.0/255.255.255.0	None (IP as username)	Add to group /		↑ ↓	×
<input checked="" type="checkbox"/>	2	Marketing	192.168.2.1-192.168.2.255	None(host name as userna...	Add to group /Marketi...	Marketing policy	↑ ↓	×
<input checked="" type="checkbox"/>	3	Subnet 1	192.168.1.0/255.255.255.0	Password based authentica...	Add to group /IT/		↑ ↓	×
-	4	Default Policy	0.0.0.0-255.255.255.255	None (IP as username)	Add to group /Default...	Default Policy	↑ ↓	×

Step 2 Click Edit Multiple. The **Edit Multiple Authentication Policies** screen is displayed. Select **Authentication**, **None/SSO**, and **Take host name as username**.

Edit Multiple Authentication Policies

Name:

☒ **Authentication**

☒ None/SSO

☐ Take IP as username

☐ Take MAC as username

☒ Take host name as username

If SSO is configured, the detected username is preferable

☐ SSO, Local or external password authentication ⓘ

The browser will be redirected to an authentication page when user attempts to access the Internet, on which user credential are required. Configure External Auth Server

☐ SSO only ⓘ

Excluded Users:

Step 5 Click Submit. The policies are successfully edited in batches.

Authentication Policy									
<input checked="" type="checkbox"/> Enable user authentication									
Authentication Zone: LAN									
+ Add ✎ Edit Multiple ✖ Delete ⬆ Move Up ⬇ Move Down 🔄 Refresh 📁 Import 📄 Example File									
<input type="checkbox"/>	No.	Name	IP/MAC	Authentication	New User Option	Description	Move	Delete	
<input type="checkbox"/>	1	SSO	192.168.3.0/255.255.255.0	None (IP as username)	Add to group /		⬆ ⬇	✖	
<input checked="" type="checkbox"/>	2	Marketing	192.168.2.1-192.168.2.255	None(host name as userna...	Add to group /Marketi...	Marketing policy	⬆ ⬇	✖	
<input checked="" type="checkbox"/>	3	Subnet 1	192.168.1.0/255.255.255.0	None(host name as userna...	Add to group /IT/		⬆ ⬇	✖	
<input type="checkbox"/>	4	Default Policy	0.0.0.0-255.255.255.255	None (IP as username)	Add to group /Default...	Default Policy	⬆ ⬇	✖	



If only Authentication is selected and edited, the new user options do not change. If only New User Option is selected and edited, the authentication mode remains unchanged.

3.7.2.1.6 Adjusting Authentication Policy Priorities

Similar to the priority of Internet access policies, the authentication policy priority is based on its serial No., the greater the serial No. is, the lower the policy priority. The NGAF verifies authentication policies from top to bottom one by one. If the IP or MAC address complies with the policy condition, the specified authentication mode is executed.

In the following figure, the condition for authentication policy Marketing Group 1 is the network segment 192.168.2.1-192.168.2.10, and that for authentication policy Marketing is the network segment 192.168.2.1-192.168.2.255. That is, the condition for Marketing conveys the condition of Marketing Group 1. In this case, users on the network segment 192.168.2.1-192.168.2.10 are authenticated against the policy Marketing.

Authentication Policy								
<input checked="" type="checkbox"/> Enable user authentication								
Authentication Zone: LAN								
+ Add Edit Multiple Delete Move Up Move Down Refresh Import Example File								
<input type="checkbox"/>	No.	Name	IP/MAC	Authentication	New User Option	Description	Move	Delete
<input type="checkbox"/>	1	Marketing	192.168.2.1-192.168.2.255	None(host name as userna...	Add to group /Marketi...	Marketing policy	↑ ↓	×
<input type="checkbox"/>	2	Marketing Group 1	192.168.2.1-192.168.2.10	None (IP as username)	Add to group /		↑ ↓	×
<input type="checkbox"/>	3	SSO	192.168.3.0/255.255.255.0	None (IP as username)	Add to group /		↑ ↓	×
<input type="checkbox"/>	4	Subnet 1	192.168.1.0/255.255.255.0	None(host name as userna...	Add to group /IT/		↑ ↓	×
<input type="checkbox"/>	5	Default Policy	0.0.0.0-255.255.255.255	None (IP as username)	Add to group /Default...	Default Policy	↑ ↓	×

If you select **Market Group 1** and click Move Up to move the policy above Market, the policy Market Group 1 obtains higher priority. In this case, users on the network segment 192.168.2.1-192.168.2.10 are authenticated against the policy Market Group 1.

Authentication Policy								
<input checked="" type="checkbox"/> Enable user authentication								
Authentication Zone: LAN								
+ Add Edit Multiple Delete Move Up Move Down Refresh Import Example File								
<input type="checkbox"/>	No.	Name	IP/MAC	Authentication	New User Option	Description	Move	Delete
<input type="checkbox"/>	1	Marketing Group 1	192.168.2.1-192.168.2.10	None (IP as username)	Add to group /		↑ ↓	×
<input type="checkbox"/>	2	Marketing	192.168.2.1-192.168.2.255	None(host name as userna...	Add to group /Marketi...	Marketing policy	↑ ↓	×
<input type="checkbox"/>	3	SSO	192.168.3.0/255.255.255.0	None (IP as username)	Add to group /		↑ ↓	×
<input type="checkbox"/>	4	Subnet 1	192.168.1.0/255.255.255.0	None(host name as userna...	Add to group /IT/		↑ ↓	×
<input type="checkbox"/>	5	Default Policy	0.0.0.0-255.255.255.255	None (IP as username)	Add to group /Default...	Default Policy	↑ ↓	×

3.7.2.1.7 Importing Authentication Policies

If you have to set many authentication policies, you can import them in CSV format. Click **Example File** to download the format file as shown in the following figure. Then edit the authentication policies in the file.

Authentication Policy								
<input checked="" type="checkbox"/> Enable user authentication								
Authentication Zone: LAN								
+ Add Edit Multiple Delete Move Up Move Down Refresh Import Example File								
<input type="checkbox"/>	No.	Name	IP/MAC	Authentication	New User Option	Description	Move	Delete
<input checked="" type="checkbox"/>	1	Marketing	192.168.2.1-192.168.2.255	None(host name as userna...	Add to group /Marketi...	Marketing policy	↑ ↓	×
<input type="checkbox"/>	2	Marketing Group 1	192.168.2.1-192.168.2.10	None (IP as username)	Add to group /		↑ ↓	×
<input type="checkbox"/>	3	SSO	192.168.3.0/255.255.255.0	None (IP as username)	Add to group /		↑ ↓	×
<input type="checkbox"/>	4	Subnet 1	192.168.1.0/255.255.255.0	None(host name as userna...	Add to group /IT/		↑ ↓	×
<input type="checkbox"/>	5	Default Policy	0.0.0.0-255.255.255.255	None (IP as username)	Add to group /Default...	Default Policy	↑ ↓	×

Example file:

#IP/MAC	Address	this field cannot be left blank; multiple entries are supported and separated from each other by half-width comma. The correct f						
# Authentication Method	filled in with IP authentication or Password authentication; being left blank means IP authentication.							
# New User Option	filled in with Added to local group or Deny Internet access or Casual account; being left blank means Added to local group							
Policy Name	Description	IP/MAC Address	Authentication	New User Option	Under Group			
policy1	policy1	200.200.20.2	IP Authen	Casual acc/				
policy1.1	policy1.1	200.200.20.2	IP Authen	Casual acc/				
policy1.2	policy1.2	200.200.20.2	IP Authen	Casual account				
policy2	policy2	00-1C-F1-09-50-1A	Deny Inte	/Default group				
policy2.1	policy2.1	200.200.20.245,200.2	Deny Inte	Default group/				
policy3	policy3	200.200.20.2	Password Authentic	Default group				
policy4	policy4	00-1C-F1-0	Password	Added to /				
policy5	policy5	00-1c-f1-0	Password	Added to /				

After the file is edited, click Import to import the file.

Authentication Options

The authentication options are used to set the user authentication configuration, including **SSO options**, **Authentication Page Redirection Options**, **MAC Address Identification Options**, and **Others**.

3.7.2.2.1 SSO Options

If you have a third-party authentication server to implement Intranet user authentication, SSO allows users authenticated by a third-party authentication pass the user authentication on the NGAF and obtain the corresponding Internet access privileges. The user names and passwords used by the NGAF for authentication are the same as those used by the third-party authentication server. The NGAF supports the following types of SSO: AD domain SSO, Proxy SSO, POP3 SSO, and Web SSO. The configuration of SSO here is basic configuration. The complete configurations in terms of users, authentication servers, and authentication modes are under **User Management**, **External Auth Server**, and **Authentication Policy**. (For details, see sections 3.6.1.3, 3.6.2.3, and 3.6.2.1.)

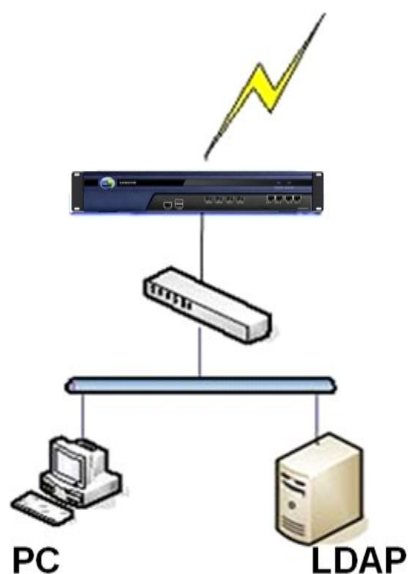
3.7.2.2.1.1 Domain SSO

If a Microsoft AD domain server is deployed on the network for user management, and the Intranet logins are managed based on the domain accounts, the domain SSO can be used. After the Intranet user logs in to the domain, the user is authenticated by the NGAF automatically. That is, the terminal user can access the Internet after the logging in to the domain. Domain SSO can be implemented by issuing domain scripts or monitoring the domain login data packets. Domain SSO is applicable only to Microsoft Active Directory (AD).

Domain SSO with domain script issuing

By issuing and executing the configured login script (logon.exe) and logoff script (logoff.exe) on the domain server at user login and logoff, user login and logoff are carried out on the NGAF.

See the following figure:



The dataflow process is as follows:

1. The PC requests for domain login.
2. The domain server turns login information to the PC.
3. The PC executes the logon.exe script and reports the domain login success information to the NGAF.

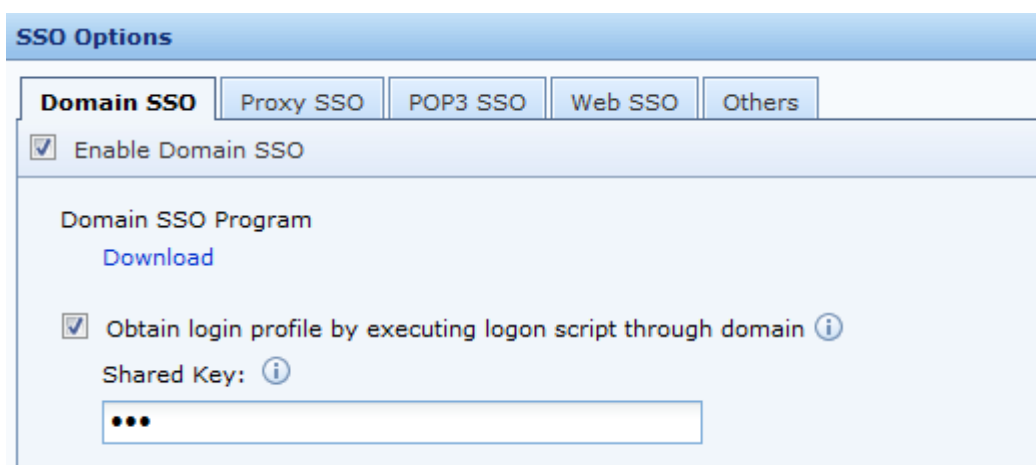
Configuration:

Step 1 Choose **User Authentication > Options > External Auth Server** and set the authentication AD domain service. (For details, see section 3.6.2.3.)

Step 2 Enable SSO, select the SSO mode, and set the shared key. Choose **User Authentication > Options > SSO Options > Domain SSO**.

Select **Enable Domain SSO**.

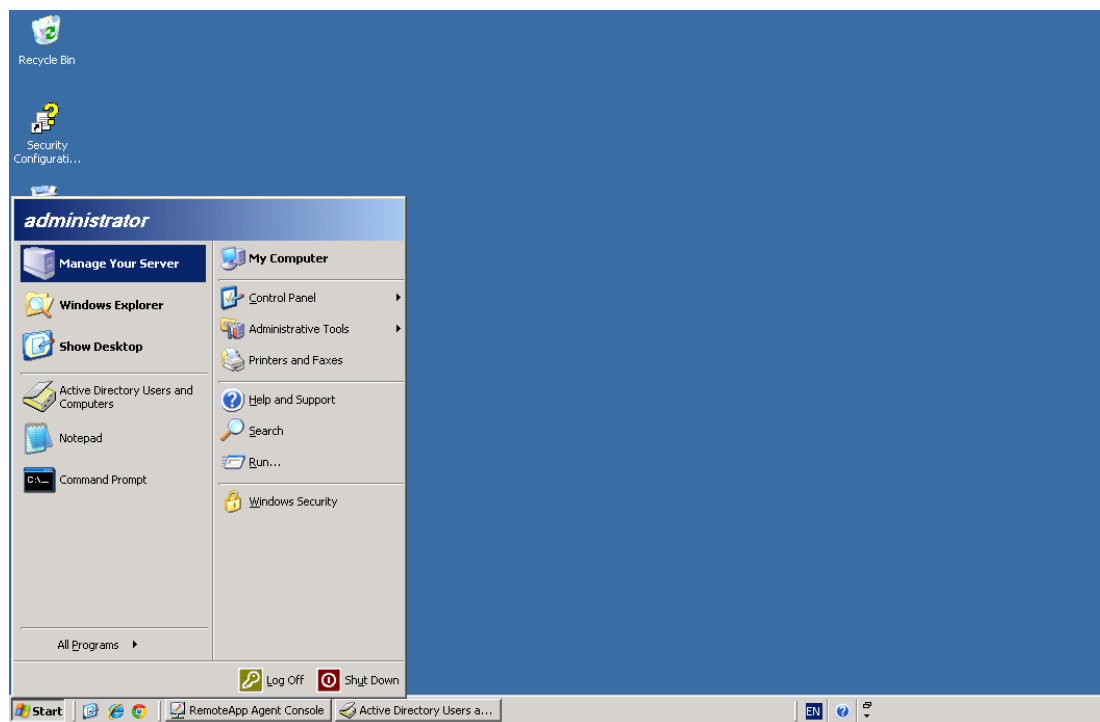
Select **Obtain login profile by executing logon script through domain**. Enter the shared key in **Shared Key**. See the following figure:



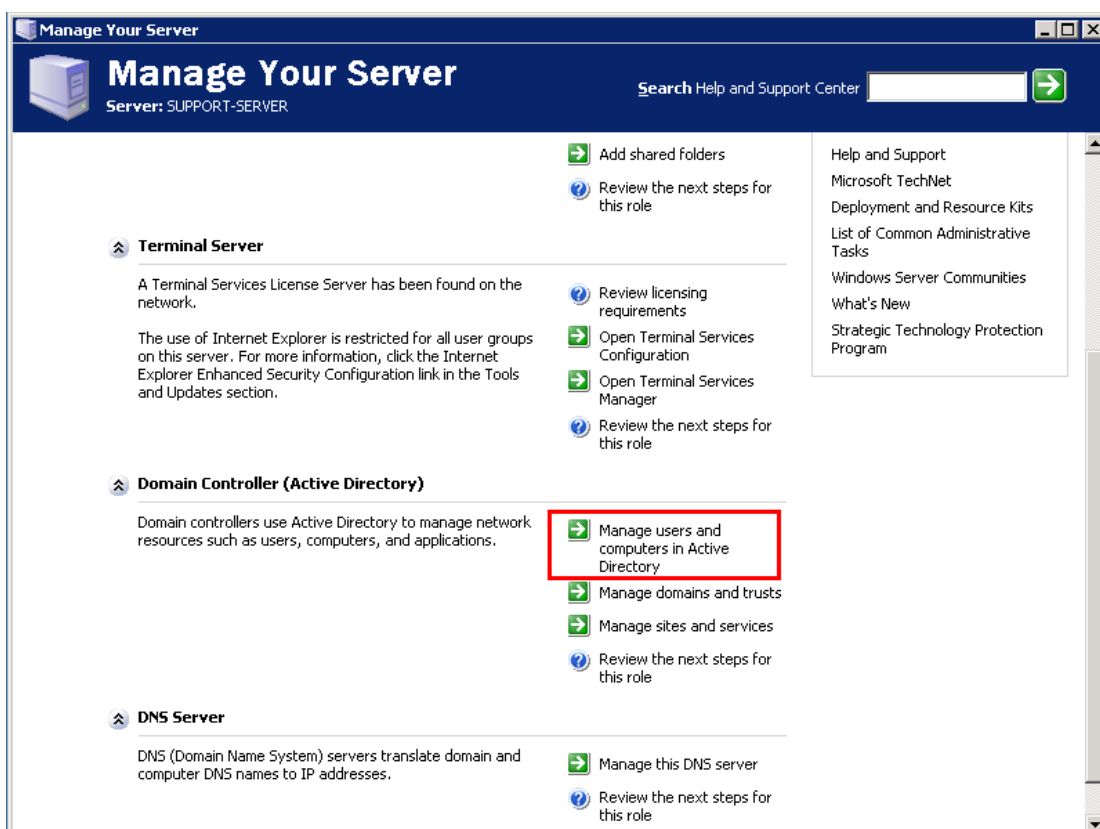
The shared key is used to encrypt the communication between the NGAF and the AD domain server, and must be specified exactly the same in the login and logoff scripts. Click Download to download the login and logoff scripts for steps 3 and 4.

Step 3 Configure the login script on the AD domain server.

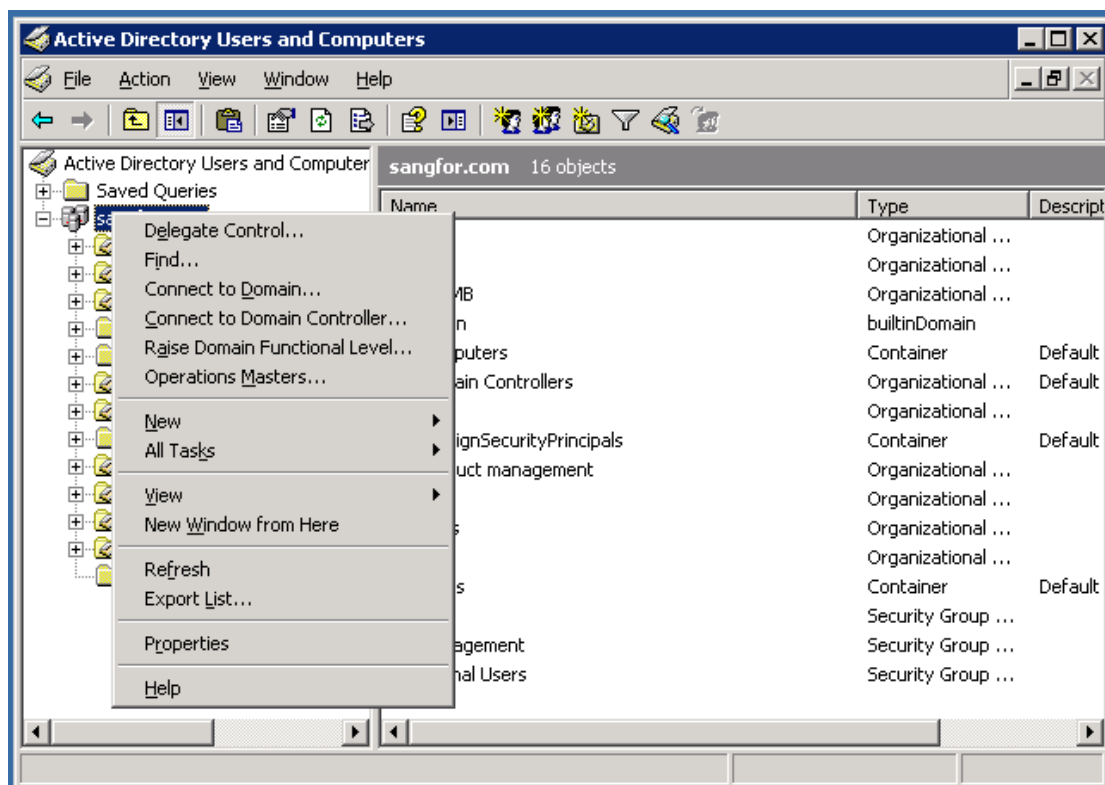
1. Log in to the domain server and choose **Manage Your Server** on the menu as shown in the following figure:



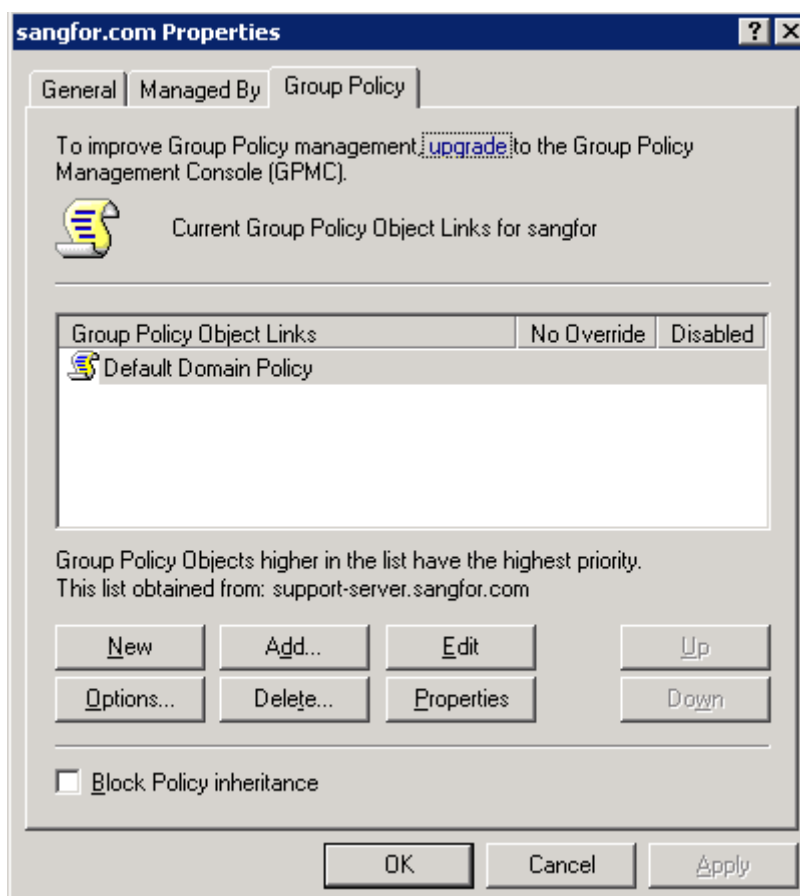
2. Click **Manage users and computers in Active Directory**. See the following figure:



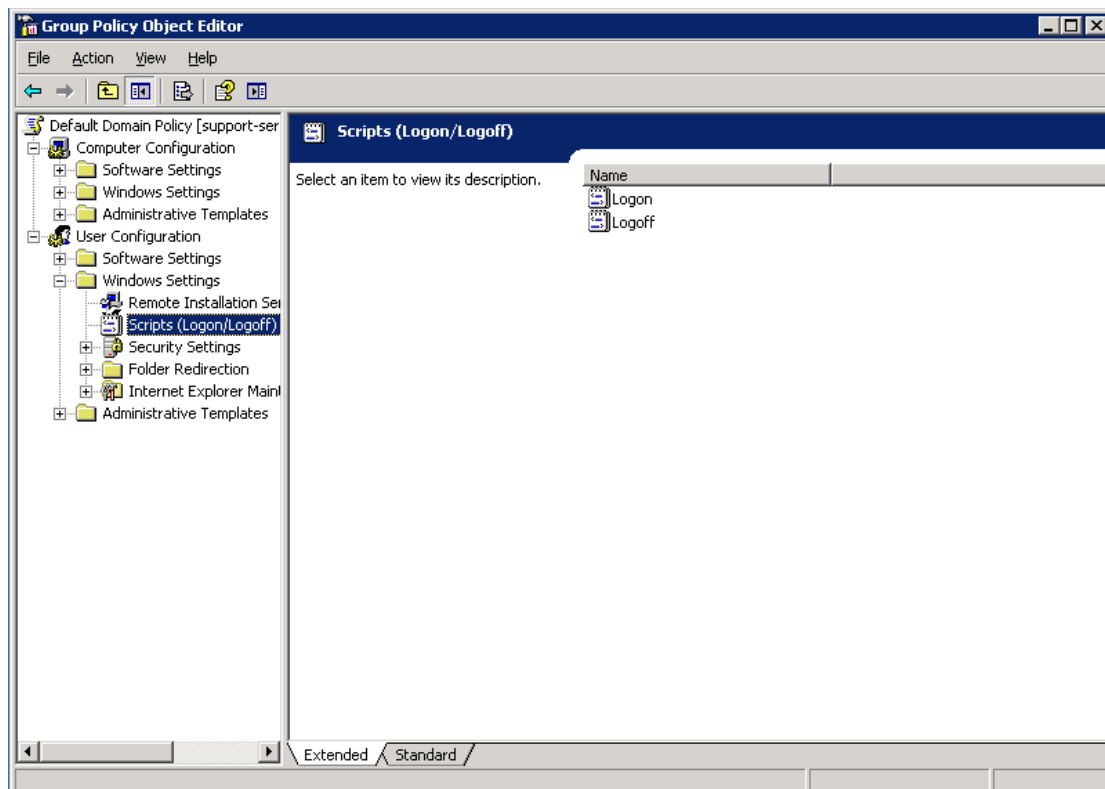
3. In the displayed window, right-click the domain to be monitored and choose **Properties**.



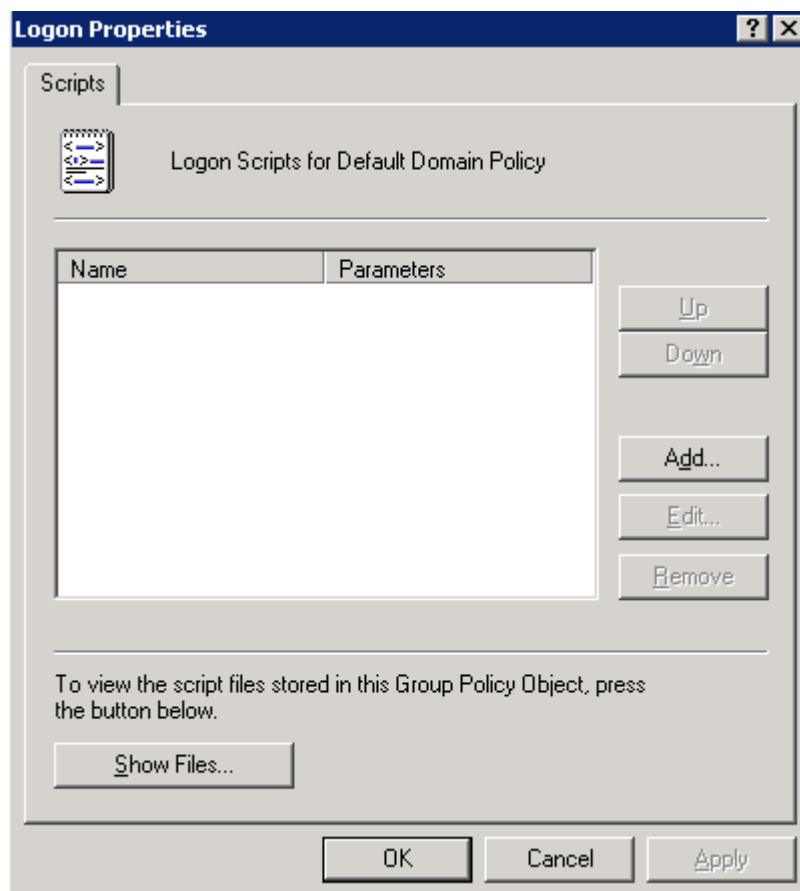
4. In the displayed window, click **Group Policy**. Double-click the group policy **Default Domain Policy**.

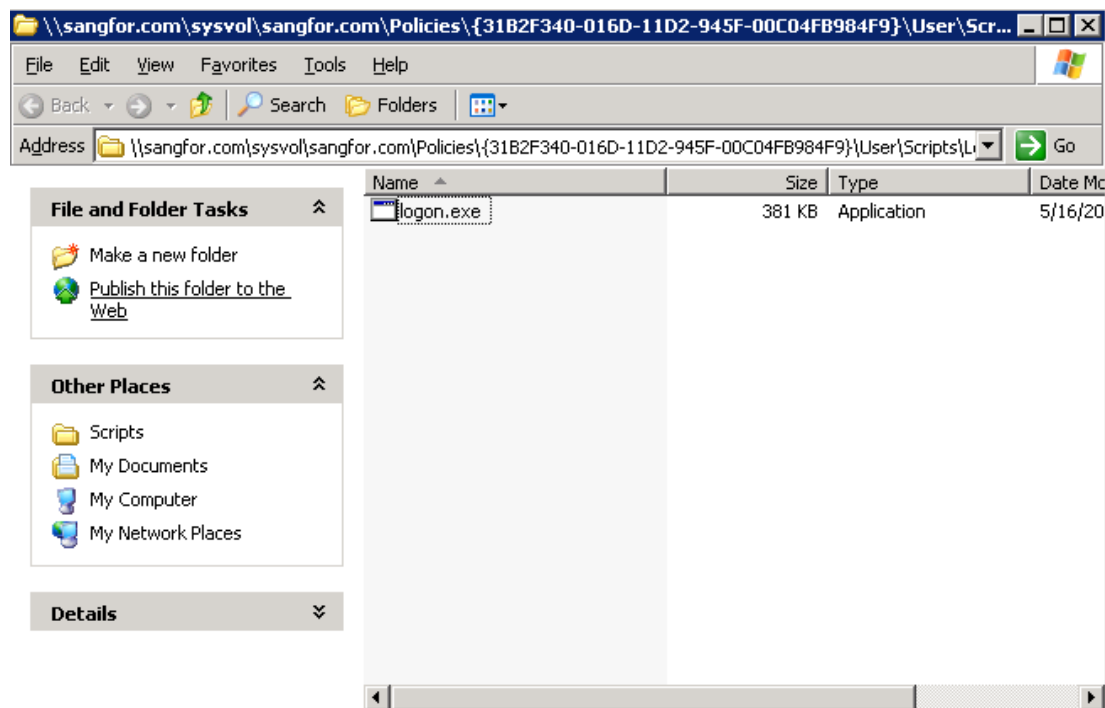


5. In the displayed **Group Policy Object Editor** window, choose **User Configuration > Windows Settings > Scripts (Logon/Logoff)**.

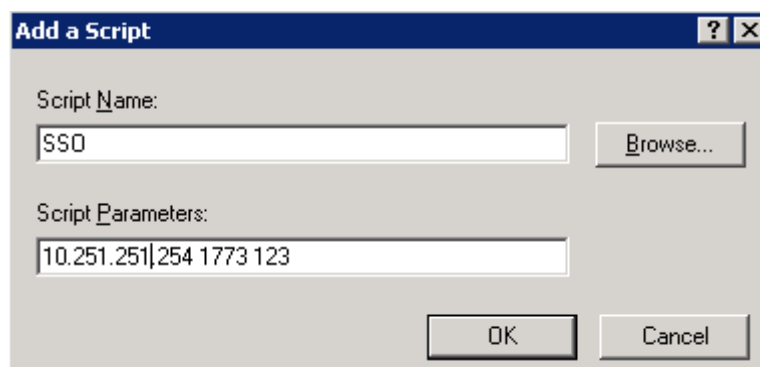


6. Double-click **Logon** on the right. In the displayed **Logon Properties** window, click **Show Files** in the lower left corner. A directory is opened. Save the login script file in the directory and close it.



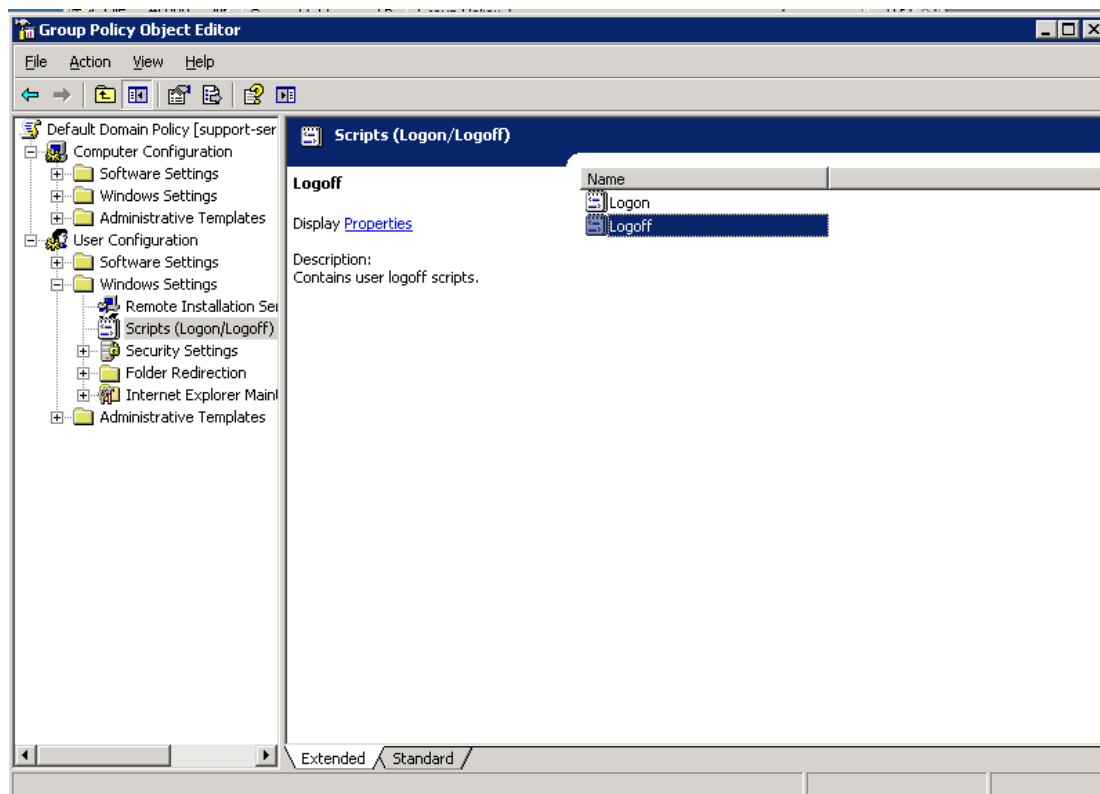


7. In the **Logon Properties** window, click **Add**. In the **Add a Script** window, click **Browse**, choose the login script file **logon.exe**, and enter the IP address (of the NGAF), port No. (fixed to 1773), and shared key (exactly the same as that configured on the NGAF) in **Script Parameters**. The parameter values must be separated by space. Click **Apply** and then **OK**. Then close the windows one by one.

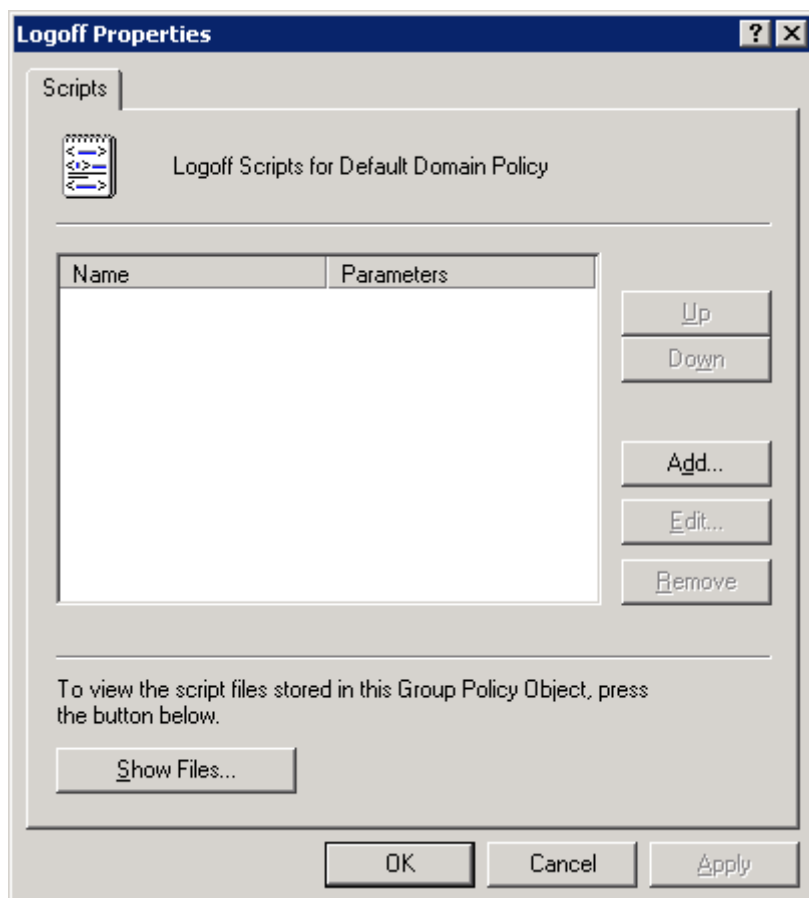


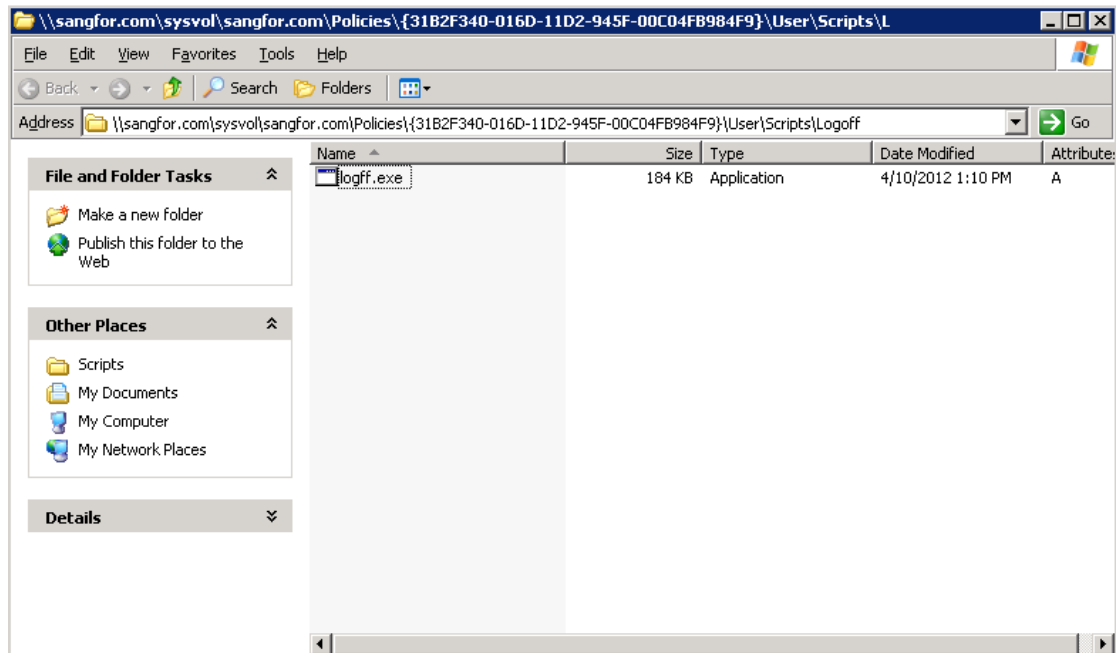
Step 4 Configure a logoff script on the AD domain server. The logoff script helps users that are logged off from the domain server log off from the NGAF as well.

1. Perform the steps for configuring the login script. In step 6, double-click **Log off** instead.

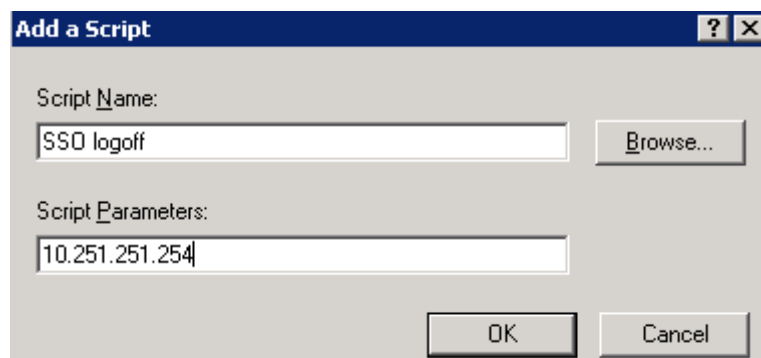


2. In the displayed **Logoff Properties** window, click **Show Files** in the lower left corner. A directory is opened. Save the logoff script file in the directory and close it.





3. In the **Logoff Properties** window, click **Add**. In the **Add a Script** window, click **Browse**, choose the logoff script file logoff.exe, and enter **Script Parameters** with the IP address of the AF exactly the same as that entered when login scrip is configured. Then close the windows one by one.



4. Choose **Start > Run**. Enter **gpupdate** and click **OK**. The group policy takes effect.

Step 5 Set the authentication policy. Choose **User Authentication > Policy**, and click **Add**. Set the authentication mode to SSO using IP or MAC addresses. (See section 3.6.2.1.3.)

Step 6 Log in to the domain on a computer and check whether you can access the Internet successfully.



- The primary DNS of the PC must be set to the IP address of the domain server. Otherwise, the domain IP address cannot be resolved, resulting in domain server login failure.
- If the DNS or IP address is changed after first successful login, the computer can log in to the computer and the domain with the correct password. However, as the Windows OS remembers the previous correct password, the login to the domain is not successful actually. Thus, the SSO fails and an

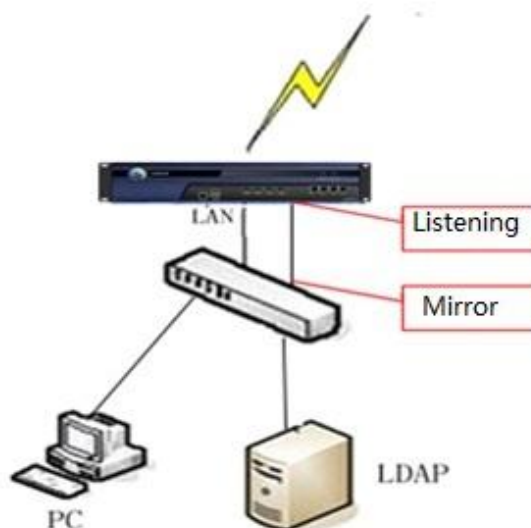
authentication dialog box requesting the user name and password is displayed when the user tries to access the Internet.

- The domain server, NGAF, and PC can be communicated properly.

Domain SSO in monitoring mode

In monitoring mode, the SSO is implemented with the user login information obtained from the data packet captured by monitoring the process of a PC logging in to the domain server. SSO in monitoring mode does not require any software to be installed on the domain server, however, requires the data packets of Intranet computers' login to the domain server pass through the NGAF, or be mirrored to the NGAF over a monitoring port. The NGAF captures the login information by monitoring the UDP 88 port. After successful login to the domain, the user can access the Internet directly, without being authenticated by the NGAF. It is applicable to scenarios where the domain server is deployed within or out of the Intranet. The SSO configurations for these two deployment modes of the domain server are described as follows:

I. Domain server deployed on the Intranet



The dataflow process is as follows:

1. The process of a PC logging in to the domain is monitored.
2. If the user logs in to the domain successfully, the NGAF authenticates the user automatically.

Configuration:

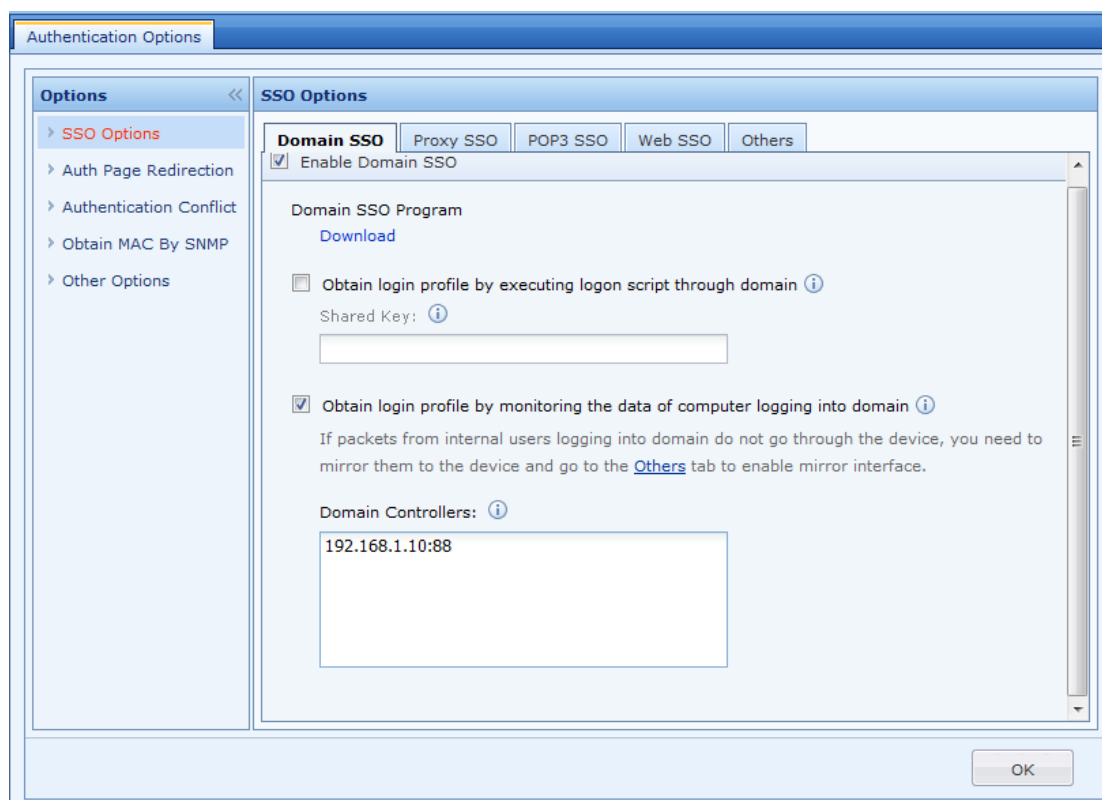
Step 1 Choose **User Authentication > Options > External Auth Server** and set the authentication AD domain service. (For details, see section 3.6.2.3.)

Step 2 Enable SSO, select the SSO mode, and set the IP address of the domain server. Choose **User Authentication > Options > SSO Options > Domain SSO**.

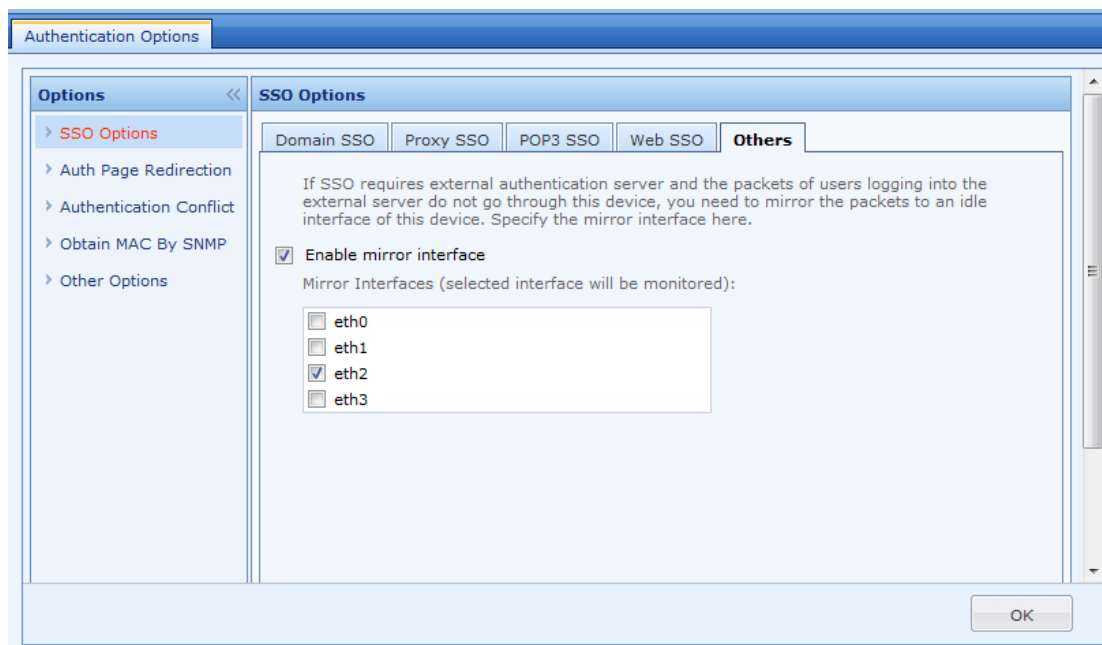
Select **Enable Domain SSO**.

Select **Obtain login profile by monitoring the data of computer logging into domain**. Enter the IP address and the monitoring port of the domain server in **Domain Controllers**. If there are multiple domain servers, enter the IP

address and the monitoring port of each domain server in one line. See the following figure:



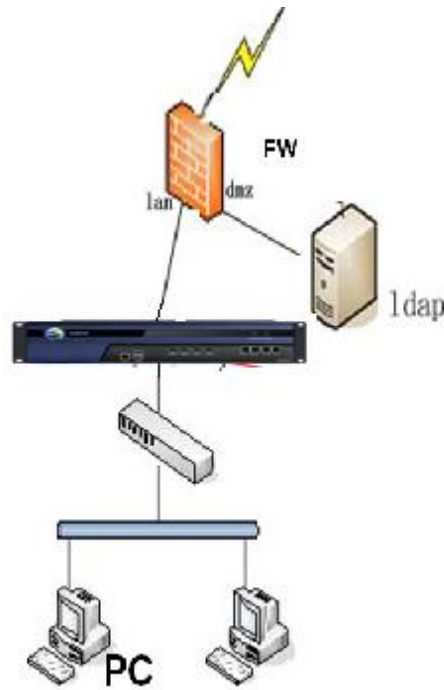
Step 3 If the login data does not pass the NGAF, set a monitoring port connected to the mirroring port on the switch forwarding login data packets. Click **Others**, and set the mirroring port. The mirroring port must be an available one not in use.



Step 4 Set the authentication policy. Choose **User Authentication > Policy**, and click **Add**. Set the authentication mode to SSO using IP or MAC addresses. (See section 3.6.2.1.3.)

Step 5 Log in to the domain on a computer and check whether you can access the Internet successfully.

I. Domain server deployed out of the Intranet



The dataflow process is as follows:

1. The data packets of a PC logging in to the domain pass through the NGAF.
2. The Intranet interface of the NGAF is used as a monitoring port.

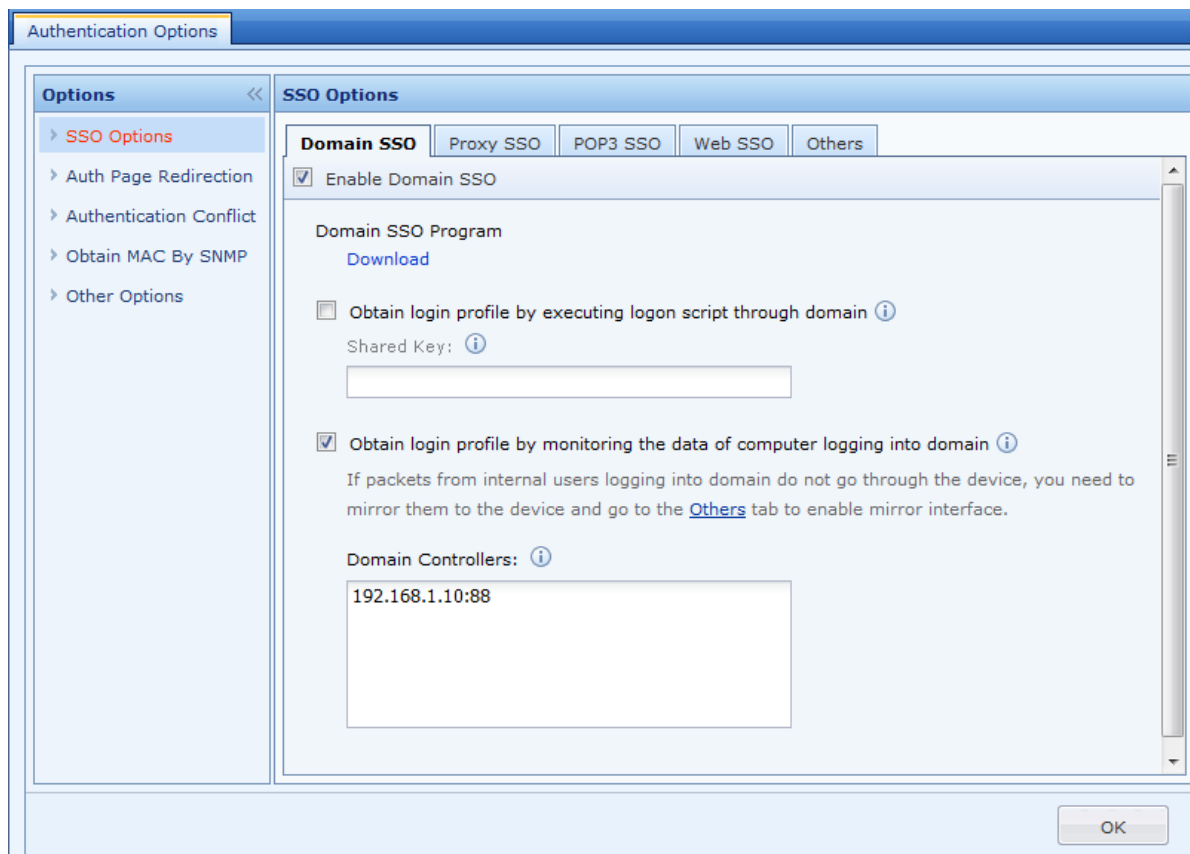
Configuration:

Step 1 Choose **User Authentication > Options > External Auth Server** and set the authentication AD domain service. (For details, see section 3.6.2.3.)

Step 2 Enable SSO, select the SSO mode, and set the IP address of the domain server. Choose **User Authentication > Options > SSO Options > Domain SSO**.

Select **Enable Domain SSO**.

Select **Obtain login profile by monitoring the data of computer logging into domain**. Enter the IP address and the listening port of the domain server in **Domain Controllers**. If there are multiple domain servers, enter the IP address and the listening port of each domain server in one line. See the following figure:



Step 3 Set the authentication policy. Choose **User Authentication > Policy**, and click **Add**. Set the authentication mode to SSO using IP or MAC addresses. (See section 3.6.2.1.3.)

Step 4 Log in to the domain on a computer and check whether you can access the Internet successfully.

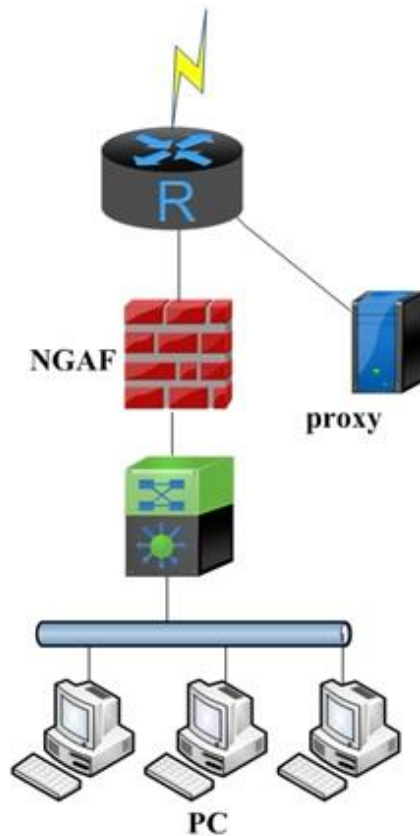


In monitoring mode, only the user login information is monitored. The logoff data is not captured.

Therefore, the logoff state is not obtained. In this case, the PC may have logged off while the user is not logged off in the online user list on the NGAF.3.6.2.2.1.2 PROXY SSO

It is applicable when users access the Internet through a proxy and each user is assigned a proxy server account. If proxy SSO is used, the users are authenticated by the NGAF when the users are authenticated by the proxy server. Proxy SSO works in monitoring mode. SSO is implemented based on login data monitoring.

Scenario 1: The proxy server is located on an external network. See the following figure:



The data flow is as follows:

1. A user accesses the Internet through the proxy server. The device monitors the interaction between the PC and proxy server.
2. When the PC is authenticated by the proxy server, it is also authenticated by the device.

Configuration:

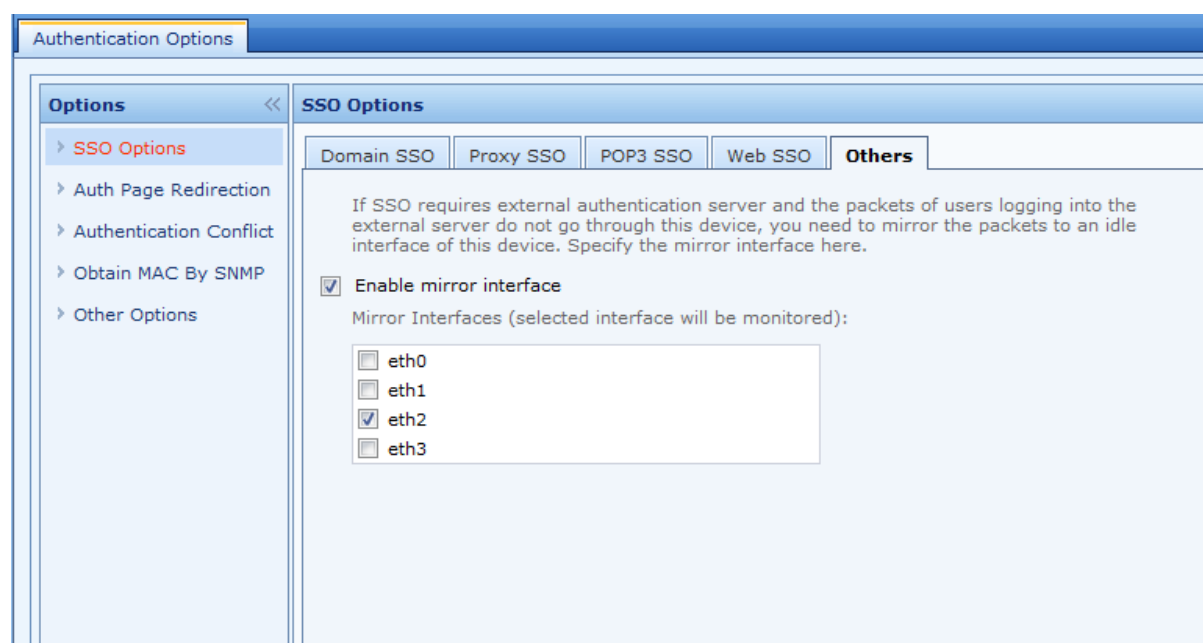
Step 1 Enable SSO on the device, select the monitoring mode, and set the IP address of the domain server. Choose **User Authentication > Options > SSO Options > Proxy SSO**.

Select **Enable Proxy SSO** to enable the proxy SSO function.

Enter the IP address and port number of the proxy server for proxy authentication in the **Proxy Server List** text box. If there are multiple IP addresses and port numbers, each line contains only one IP address and port number. See the following figure:



Step 2 If login data is not transferred through the device. You must set a mirror interface and connect it to the mirror interface of the switch that forwards login data. Click **Others** and set the mirror interface. The mirror interface must be an idle network interface.



Step 3 Set authentication policies based on the IP addresses or MAC addresses of the users who require proxy SSO. Choose **User Authentication > Policy**, click **Add**, and set the policies. (See section 3.6.2.1.3.)

Step 4 Log in to the proxy server on the PC. You can access the Internet after successful login.



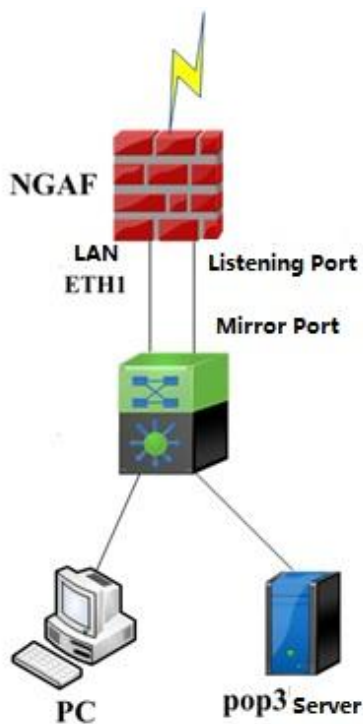
If the proxy server is located on an external network while automatic authentication is required, you must assign the permission in the root group to access the proxy server. (For configuration details, see section 3.8.1.) In addition, choose **Authentication Options > Other Options**, and select **Basic services (except HTTP)** are available before user passes authentication. See the following figure:

Authentication Options	
Options << <ul style="list-style-type: none"> > SSO Options > Auth Page Redirection > Authentication Conflict > Obtain MAC By SNMP > Other Options 	Other Options <ul style="list-style-type: none"> <input type="checkbox"/> Auto logout the user who causes no flow in a specified period Time Period (mins): <input type="text" value="120"/> ⓘ <input type="checkbox"/> Submit user credential using POST method <input checked="" type="checkbox"/> DNS service is available before user passes authentication <input checked="" type="checkbox"/> Basic services (except HTTP) are available before user passes authentication <input type="checkbox"/> Require authentication again if MAC address is changed <input type="checkbox"/> Lock user if authentication attempts reaches the threshold ⓘ Max Attempts: <input type="text" value="2"/> Lockout Period (mins): <input type="text" value="1"/> ⓘ

3.7.2.2.1.3 POP3 SSO

There is an email server on a customer's network and user information is stored on the POP3 server. Before accessing the Internet, a user uses a client such as Outlook or Foxmail to log in to the POP3 server to send and receive emails. When the device working in monitoring mode detects user login, it identifies and authenticates the user. Then, the user can access the Internet without entering a user name and password another time. This is applicable regardless of whether the POP3 server is located on an internal or external network. The methods of configuring POP3 SSO for the two scenarios are described as follows:

Scenario 1: The POP3 server is located on an intranet.



The data flow is as follows:

1. The user initiates communication with the POP3 server by using an email client. The device monitors the communication.
2. When the email client successfully logs in to the POP3 server, the device authenticates the user. Therefore, the user can access the Internet without entering a password again.
3. Because data is exchanged on the intranet, POP3 login data is not transferred to the devices. Therefore, a monitor interface must be set on the device.

Configuration:

Step 1 Set the POP3 server for authentication. Choose **User Authentication > Options > External Auth Server**. (For details, see section 3.6.2.3.)

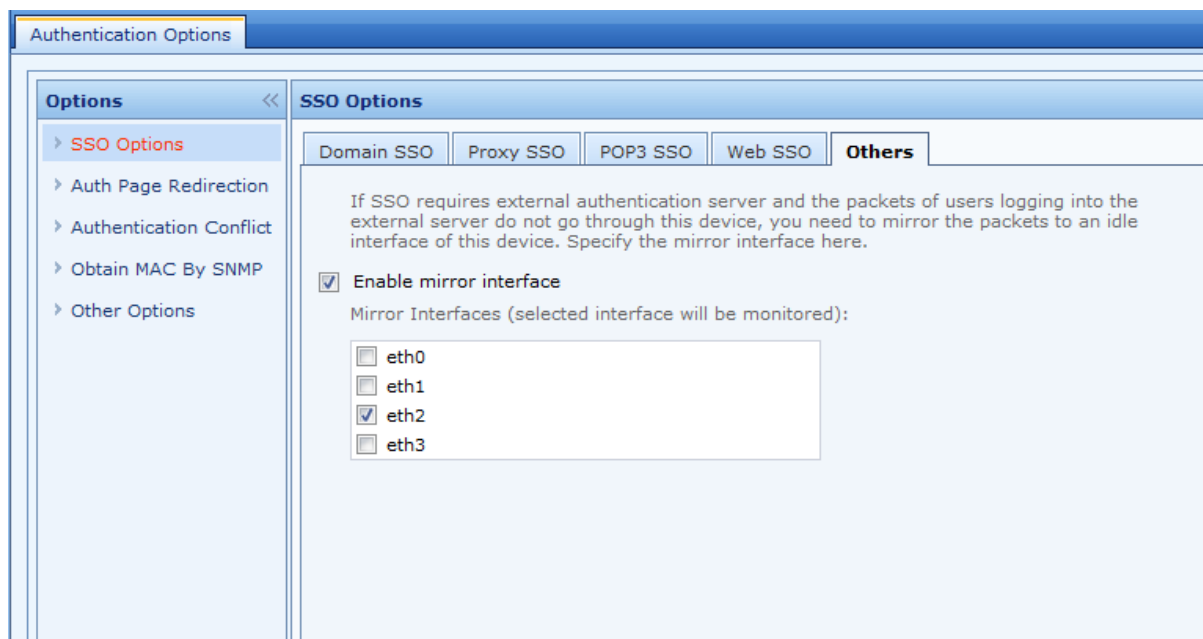
Step 2 Enable SSO on the device, select the monitoring mode, and set the IP address of the domain server. Choose **User Authentication > Options > SSO Options > POP3 SSO**.

Select **Enable POP3 SSO** to enable the POP3 SSO function.

Enter the IP address and port number (default port number: TCP110) of the POP3 server for POP3 authentication in the **Mail Server List** text box. If there are multiple IP addresses and port numbers, each line contains only one IP address and port number. See the following figure:



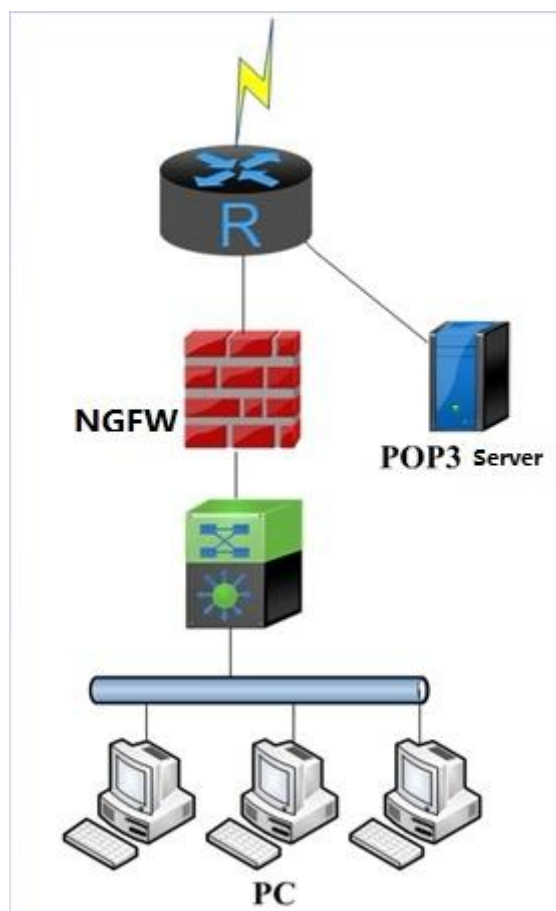
Step 3 If login data is not transferred through the device. You must set a mirror interface and connect it to the mirror interface of the switch that forwards login data. Click **Others** and set the mirror interface. The mirror interface must be an idle network interface.



Step 4 Set authentication policies based on the IP addresses or MAC addresses of the users who require POP3 SSO. Choose **User Authentication** > **Policy**, click **Add**, and set the policies. (See section 4.6.2.1.3.)

Step 5 Send and receive emails using an email client on the PC. After POP3 server login is successful, you can access the Internet.

Scenario 2: The POP3 server is located on an external network.



The data flow is as follows:

1. Login data is transferred from the PC through the device to the POP3 server.
2. The intranet interface of the device is also used as the monitor interface. Therefore, no more monitor interface needs to be set.

Configuration:

Step 1 Set the POP3 server for authentication. Choose **User Authentication > Options > External Auth Server**. (For details, see section 4.6.2.3.)

Step 2 Enable SSO on the device, select the monitoring mode, and set the IP address of the domain server. Choose **User Authentication > Options > SSO Options > POP3 SSO**.

Select **Enable POP3 SSO** to enable the POP3 SSO function.

Enter the IP address and port number (default port number: TCP110) of the POP3 server for POP3 authentication in the **Mail Server List** text box. If there are multiple IP addresses and port numbers, each line contains only one IP address and port number. See the following figure:



Step 3 Set authentication policies based on the IP addresses or MAC addresses of the users who require POP3 SSO. Choose **User Authentication > Policy**, click **Add**, and set the policies. (See section 4.6.2.1.3.)

Step 4 Send and receive emails using an email client on the PC. After POP3 server login is successful, you can access the Internet.



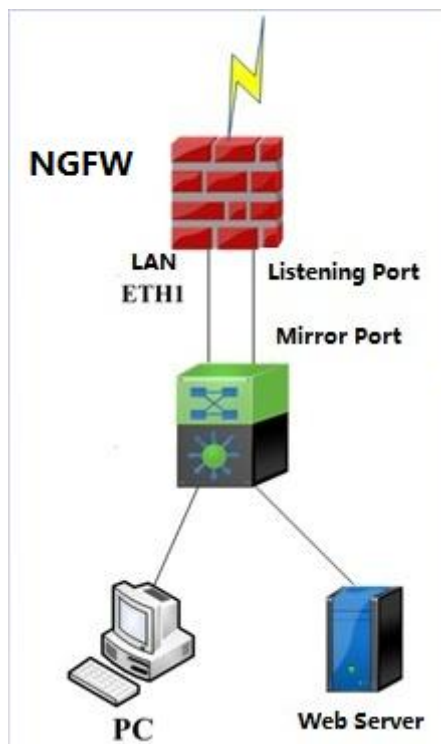
If the POP3 server is located on an external network while automatic authentication is required, you must assign the permission in the root group to access the POP3 server. (For configuration details, see section 4.8.1.) In addition, choose Authentication Options > Other Options, and select Basic services (except HTTP) are available before user passes authentication. See the following figure:

Authentication Options	
Options << <ul style="list-style-type: none"> > SSO Options > Auth Page Redirection > Authentication Conflict > Obtain MAC By SNMP > Other Options 	Other Options <ul style="list-style-type: none"> <input type="checkbox"/> Auto logout the user who causes no flow in a specified period Time Period (mins): <input type="text" value="120"/> ⓘ <input type="checkbox"/> Submit user credential using POST method <input checked="" type="checkbox"/> DNS service is available before user passes authentication <input checked="" type="checkbox"/> Basic services (except HTTP) are available before user passes authentication <input type="checkbox"/> Require authentication again if MAC address is changed <input checked="" type="checkbox"/> Lock user if authentication attempts reaches the threshold ⓘ Max Attempts: <input type="text" value="2"/> Lockout Period (mins): <input type="text" value="1"/> ⓘ

3.7.2.2.1.4 Web SSO

Web SSO is applicable to users who have their own web servers and the web servers store account information. When the users are authenticated by the web servers, they are also authenticated by the device. This is applicable regardless of whether the web server is located on an internal or external network.

Scenario 1: The web server is located on an intranet.



The data flow is as follows:

1. A user logs in to the web server. Data is transferred in plain text during the process. The device monitors the

communication.

2. The device determines whether the user is authenticated by the web server based on the keyword sent back from the server. If the user is authenticated by the web server, the device authenticates the user.

Configuration:

Step 1 Enable SSO on the device, select the monitoring mode, and set the shared secret. Choose **User and Policy Management > User Authentication > Authentication Options** on the **Policy Navigation** page. Authentication options are displayed on the right. Choose **SSO Options > Web SSO**, and select **Enable Web SSO**.

The screenshot shows the 'Authentication Options' configuration page. On the left, there is a sidebar with 'Options' and 'SSO Options' sections. The 'SSO Options' section is active, showing tabs for 'Domain SSO', 'Proxy SSO', 'POP3 SSO', 'Web SSO', and 'Others'. The 'Web SSO' tab is selected. The main content area for 'Web SSO' includes a checkbox labeled 'Enable Web SSO' which is checked. Below this, there is a text box for 'Web Authentication Server' with the value 'bbs.sangfor.com'. There is also a checkbox for 'Redirect browser to the above server before authentication' which is checked. A text box for 'User Form Name' contains the value 'pwuser'. At the bottom, there are two radio buttons: 'Authentication success keyword' (selected) and 'Authentication failure keyword'.

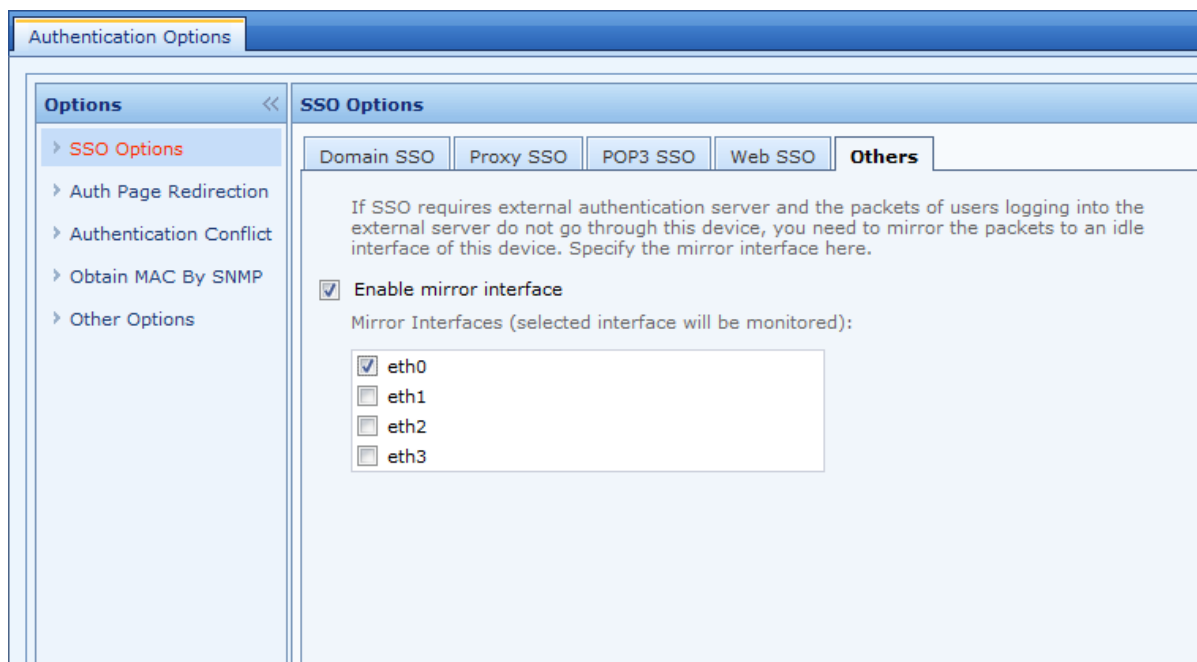
Step 2 Enter the address of the web authentication server in the **Web Authentication Server** text box.

Step 3 Select **Redirect browser to the above server before authentication**. When a user is not authenticated, the user is redirected to the page for web SSO when the user accesses any page.

Step 4 Enter the name of the list containing the user names to be submitted to the server during web authentication in the **User Form Name** text box.

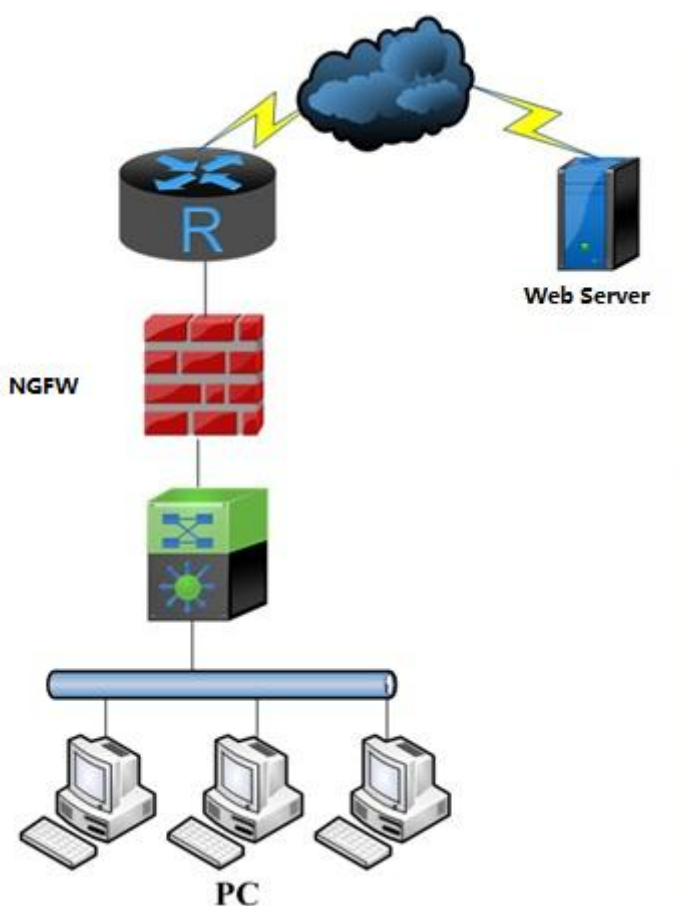
Step 5 Select **Authentication success keyword** or **Authentication failure keyword** and enter the keyword indicating whether web server login is successful. For example, if you have selected **Authentication success keyword** and enter a keyword and the keyword is contained in the POST response, web SSO is successful. If you have selected **Authentication failure keyword** and enter a keyword and the keyword is contained in the POST response, web SSO fails; otherwise, it is successful.

Step 6 Set the monitor interface. Click **Others**, select **Enable mirror interface**, and select an interface.



Step 7 Before accessing the Internet, log in to the preset website, such as the BBS website in the example. You can access the Internet after the login is successful.

Scenario 2: The web server is located on an external network.



The data flow is as follows:

1. Login data is transferred from the PC through the device to the web server.

2. The intranet interface of the device is also used as the monitor interface. Therefore, no more monitor interface needs to be set. Web SSO is successful when web server login is successful.

Configuration:

Step 1: Enable SSO on the device, select the monitoring mode, and set the shared secret. Choose **User and Policy Management > User Authentication > Authentication Options** on the **Policy Navigation** page. Authentication options are displayed on the right. Choose **SSO Options > Web SSO**, and select **Enable Web SSO**.

The screenshot shows the 'Authentication Options' configuration page. On the left, there is a sidebar with 'Options' and 'SSO Options' expanded. The main area is titled 'SSO Options' and contains several tabs: 'Domain SSO', 'Proxy SSO', 'POP3 SSO', 'Web SSO' (selected), and 'Others'. Under the 'Web SSO' tab, there is a checkbox labeled 'Enable Web SSO' which is checked. Below this, there is a text box for 'Web Authentication Server' with the value 'bbs.sangfor.com'. There is also a checkbox labeled 'Redirect browser to the above server before authentication' which is checked. Below that, there is a text box for 'User Form Name' with the value 'pwuser'. At the bottom, there are two radio buttons: 'Authentication success keyword' (selected) and 'Authentication failure keyword'.

Step 2 Enter the address of the web authentication server in the **Web Authentication Server** text box.

Step 3 Select **Redirect browser to the above server before authentication**. When a user is not authenticated, the user is redirected to the page for web SSO when the user accesses any page.

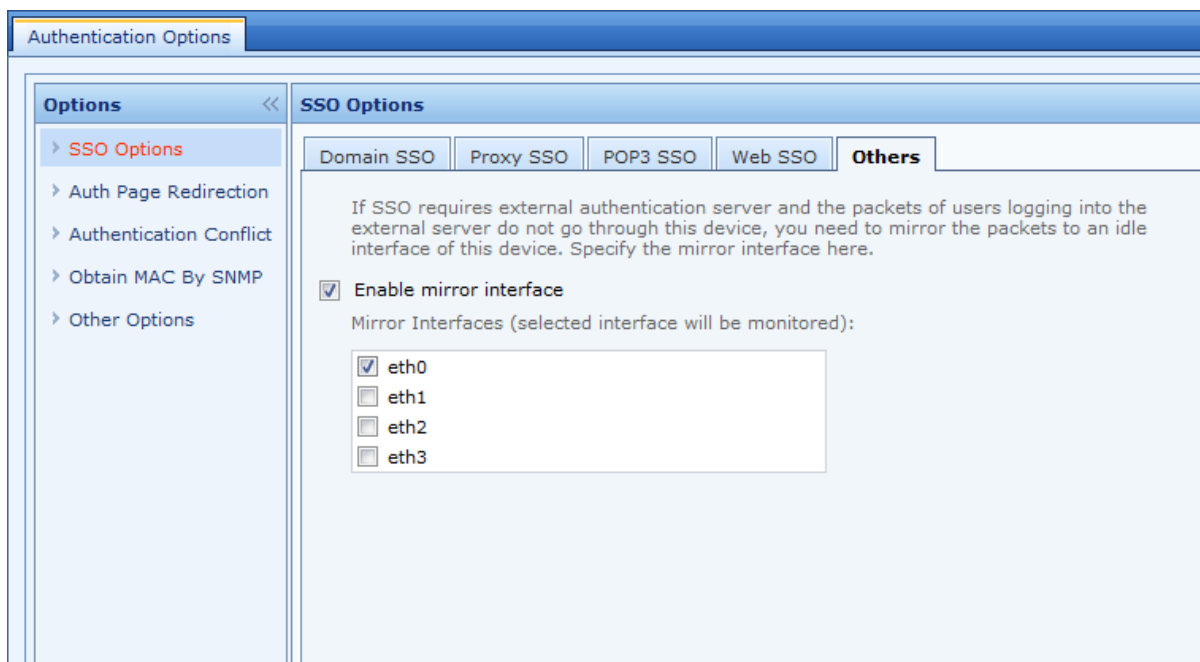
Step 4 Enter the name of the list containing the user names to be submitted to the server during web authentication in the **User Form Name** text box.

Step 5 Select **Authentication success keyword** or **Authentication failure keyword** and enter the keyword indicating whether web server login is successful. For example, if you have selected **Authentication success keyword** and enter a keyword and the keyword is contained in the POST response, web SSO is successful. If you have selected **Authentication failure keyword** and enter a keyword and the keyword is contained in the POST response, web SSO fails; otherwise, it is successful.

Step 6 Before accessing the Internet, log in to the preset website, such as the BBS website in the example. You can access the Internet after the login is successful.

3.7.2.2.1.5 Other Options

If server login data is not transferred through the gateway, you need to select a mirror interface on the **Others** tab page as the monitor interface. This monitor interface is required for domain SSO, POP3 SSO, and web SSO.



3.7.2.2.2 Redirection After Successful Authentication

Auth Page Redirection is used to specify the page to which a user is redirected after successful web authentication. See the following figure:

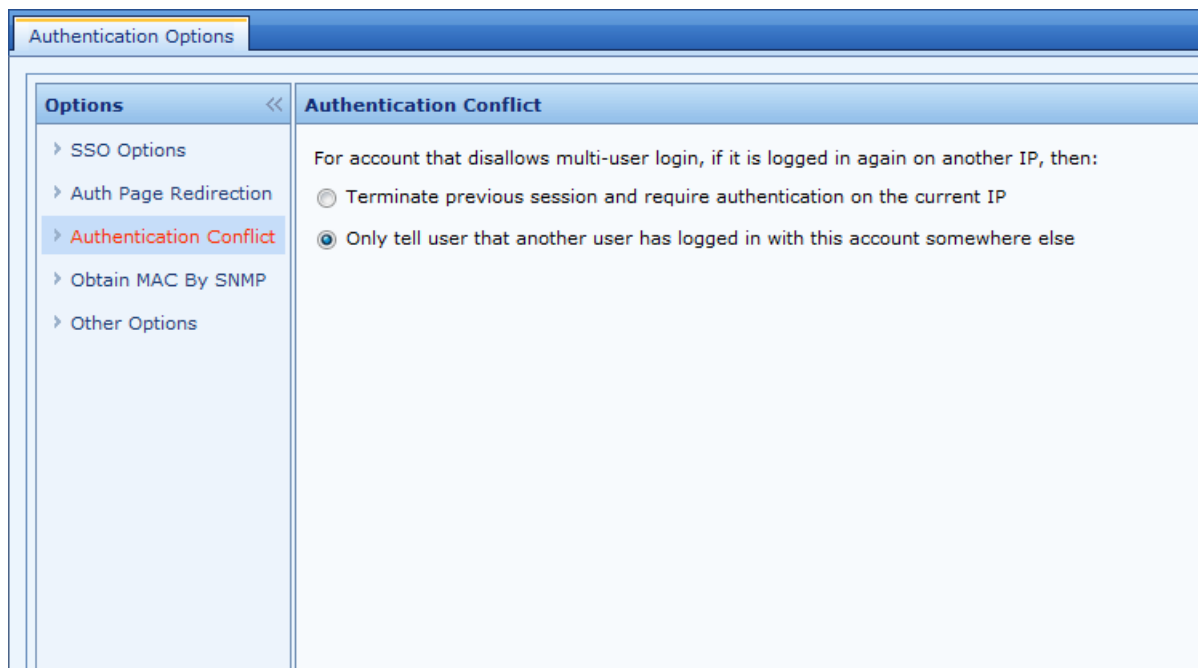
If you select **Recently visited page**, an intranet user is redirected to the originally requested page after successful authentication.

If you select **Logout page**, an intranet user is redirected to the manual logout page after successful authentication.

If you select **Specified page**, an intranet user is redirected to the page specified by the user after successful authentication.

3.7.2.2.3 Authentication Conflict

Authentication Conflict is used to disallow multiple users to use the same account at the same time to log in. The device handles the conflict either by terminating the previous session and requiring authentication on the current IP address or only by telling the user that another user has logged in with the same account somewhere else. See the following figure:



3.7.2.2.4 IP or MAC Address Identification Across Three Layers

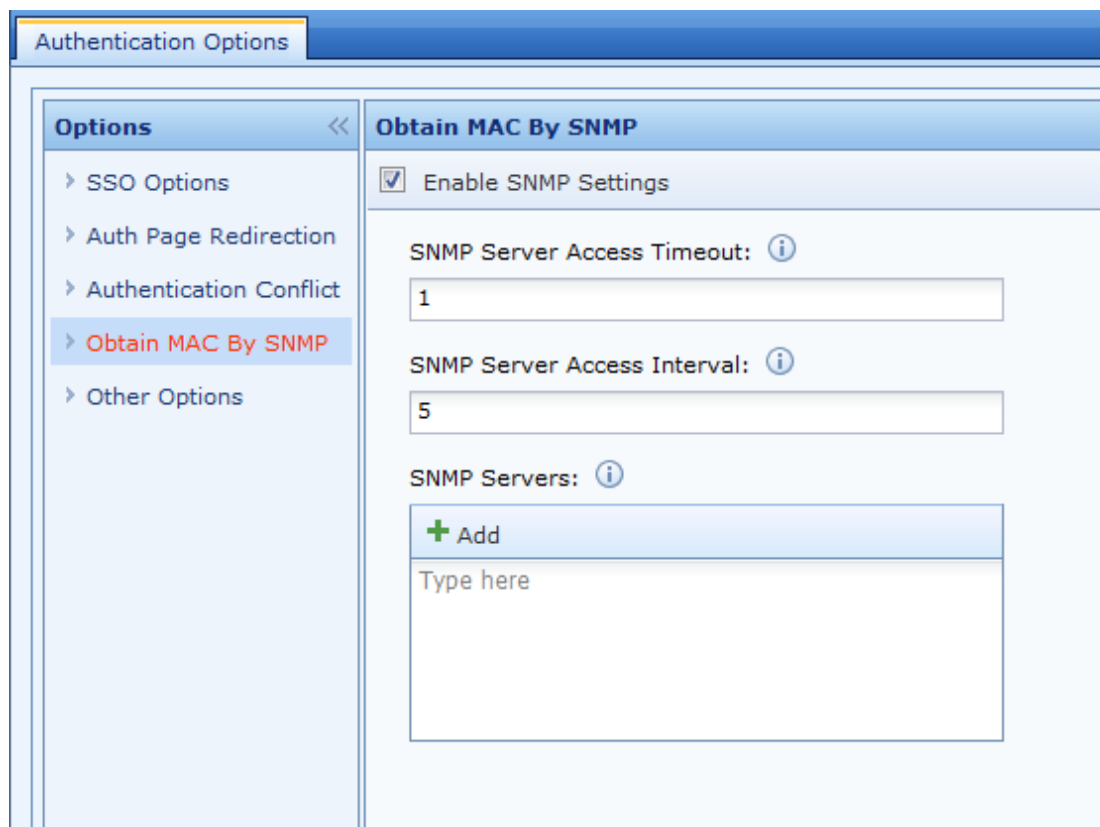
If intranet users bind MAC addresses or only MAC address authentication is allowed and the internet network consists of three layers, **Obtain MAC by SNMP** must be enabled for obtaining MAC addresses of intranet users. This function can be used only when the switches on the intranet support the SNMP function.

Principle: The device regularly sends an SNMP request to the layer-3 switch for the MAC address table and saves it in its memory. If a computer, such as the PC with the IP address 192.168.1.2 (in a network segment different from the LAN ports of the device), connected to the layer-3 switch accesses the Internet through the device, the device determines that the MAC address of the data packets from the PC is a layer-3 MAC address. The device does not process the MAC address. Instead, it searches the memory for the real MAC address based on the IP address 192.168.1.2 and then authenticates the user based on the real MAC address.

Configuration:

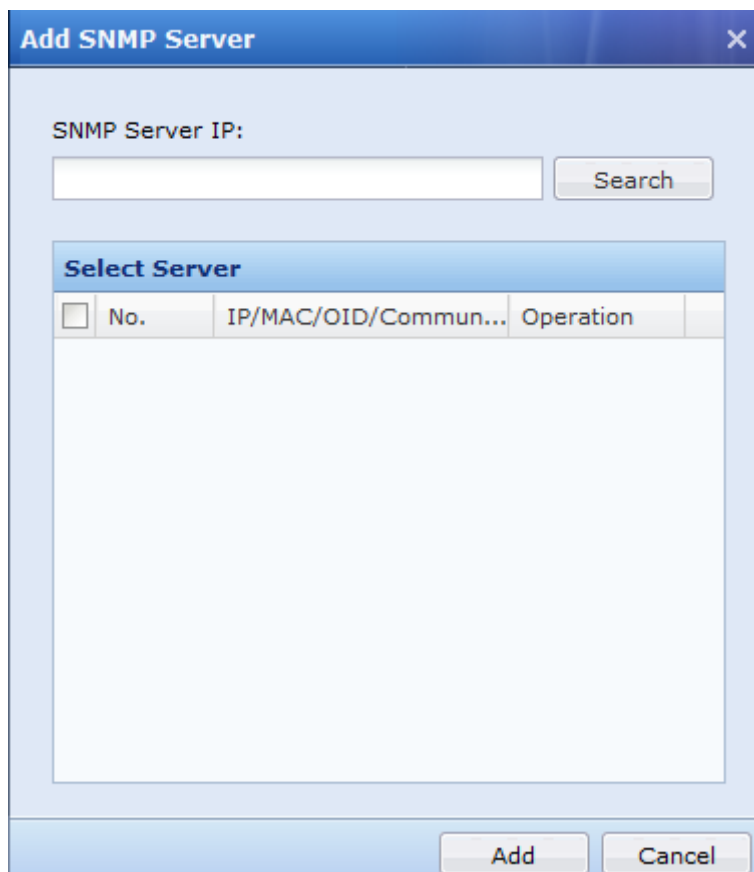
Step 1 Enable the SNMP function on the layer-3 switch.

Step 2 Choose **User Authentication > Options > Obtain MAC By SNMP**, and select **Enable SNMP Settings**.



Step 3 Set **SNMP Server Access Timeout** and **SNMP Server Access Internal**. Usually, the default values are retained.

Step 4 In the **SNMP Servers** text box, click **Add**. The **Add SNMP Server** dialog box appears. Enter the SNMP server IP address and click **Search**. Select the server found and click **Add**. See the following figure:



Step 5 Set authentication policies based on the IP addresses or MAC addresses of the users who require MAC address authentication. Choose **User Authentication > Policy**, click **Add**, and set the policies. (See section 4.6.2.1.3.)

Step 6 After the previous five steps, the computer connected to the layer-3 switch can be authenticated as a new user and access the Internet through the device.



When the SNMP server is searched for by its IP address, the SNMP function of the server must be enabled and **COMMUNITY** must be set to **Public**. Otherwise, the search fails and you need to enter SNMP server information manually.

3.7.2.2.5 Other Authentication Options

Other Options is used to set some options related to authentication. See the following figure:

You can select **Auto logout the user who causes no flow in a specified period** and set a timeout interval. If a user causes no flow within the specified interval, the user is logged out.

You can select **Submit user credential using POST method** so that an authentication web page is displayed when a user uses a user name and password for authentication.

You can select **DNS service is available before user passes authentication** to allow users to access the DNS service before being authenticated.

You can select **Basic services (except HTTP) are available before user passes authentication** to assign, before users are authenticated, root group permissions to the users except the permission to use the HTTP service.

You can select **Require authentication again if MAC address is changed** to require re-authentication of a user who has been authenticated before when the MAC address of the user is changed. For example, if the user whose IP address is 192.168.1.1 has been authenticated using a user name and password, the user is not deregistered in a certain period after the user logs out. If another user changes his or her IP address to 192.168.1.1, this means that

the IP address corresponds to another MAC address. In this case, re-authentication is required.

You can select **Lock user if authentication attempts reaches the threshold** to specify the maximum number of consecutive authentication failures and the user locking duration. The figure shows that a user is locked for 1 minute after three consecutive login failures.



1. In authentication mode that requires a user name and password, a user can change the password without the help of the administrator. If the change fails, the account of the user is locked for the period specified by **Lock user if authentication attempts reaches the threshold**.
2. Access <http://device IP address>, click **Change Password**. The password change page appears.

Modify Password

Username:

Current Password:

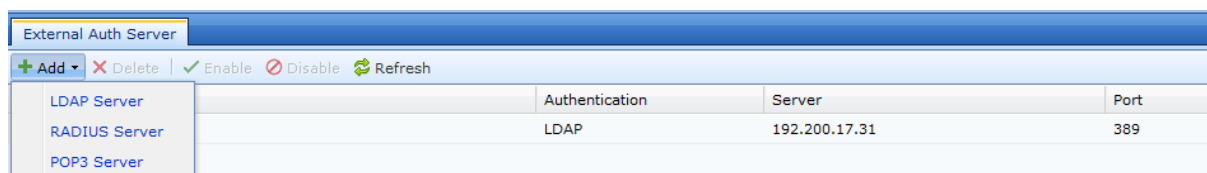
New Password:

Confirm Password:

Enter the user name whose password is to be changed, old password, and new password, confirm the new password, and click **Submit**.

External Authentication Server

External Auth Server is used to configure information about third-party authentication servers. The device support LDAP, RADIUS, and POP3 external authentication servers. Click **Add**. A drop-down list box appears.



3.7.2.3.1 Adding an External Authentication Server

Adding an LDAP Server

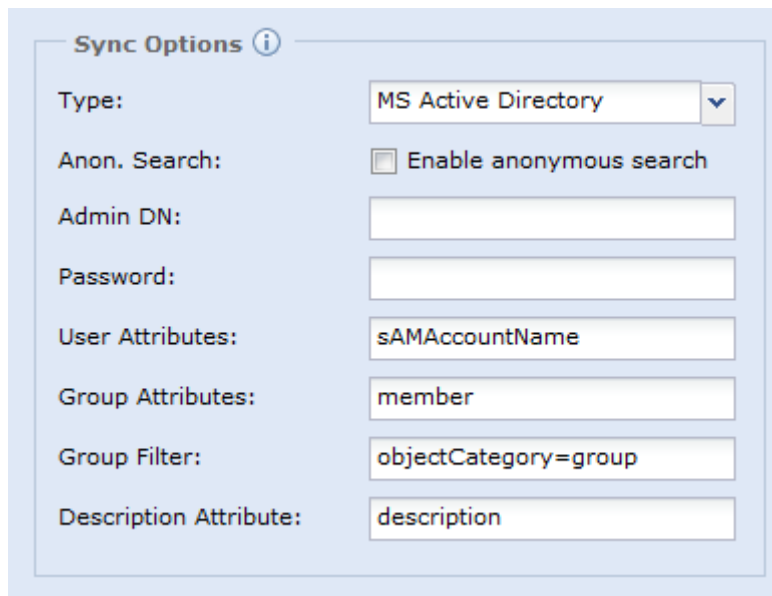
Choose **User and Policy Management** on the navigation page. Choose **User Authentication** > **External Auth Server**. On the **External Auth Server** page, click **Add** and choose **LDAP Server**. The **External Authentication Server (LDAP)** page appears.

In the **Basic Settings** area, set a server name, server IP address, authentication port, timeout interval, and BaseDN (path of the server where the user resides).

The screenshot shows the 'Basic Settings' form for adding an LDAP server. It contains the following fields:

- Server Name:** A text input field.
- Server Address:** A text input field.
- Port:** A text input field with the value '389'.
- Timeout(sec):** A text input field with the value '5'.
- Base DN:** A text input field with a dropdown arrow on the right.

In the **Sync Options** area, enter a user name and password of a domain user and select the type of the domain. The following five types are supported: **MS Active Directory**, **OPEN LDAP**, **SUN LDAP**, **IBM LDAP**, and **OTHER LADAP**.



Sync Options ⓘ

Type: MS Active Directory ▼

Anon. Search: ☐ Enable anonymous search

Admin DN:

Password:

User Attributes: sAMAccountName

Group Attributes: member

Group Filter: objectCategory=group

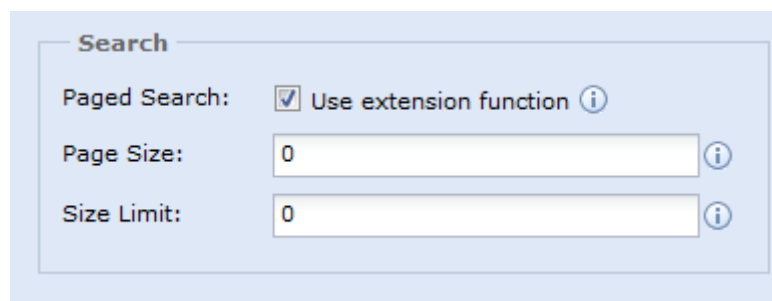
Description Attribute: description

Search configuration:

You can select **Use extension function** if the LDAP server supports paged search. Otherwise, use ordinary LDAP search. Usually, the server does not support paged search because the function has been disabled on the server or the LDAP software does not support the function, such as early versions of OpenLDAP.

Page Size indicates the size of content on each search result page when the extension function is used to search. You can consult the LDAP server administrator. (Usually, the values 800, 400, 200, and so on are used. You can try a smaller value until synchronization can be implemented.)

Size Limit is related to synchronization. Do not set this parameter unless the server has the requirement.



Search

Paged Search: ☒ Use extension function ⓘ

Page Size: 0 ⓘ

Size Limit: 0 ⓘ

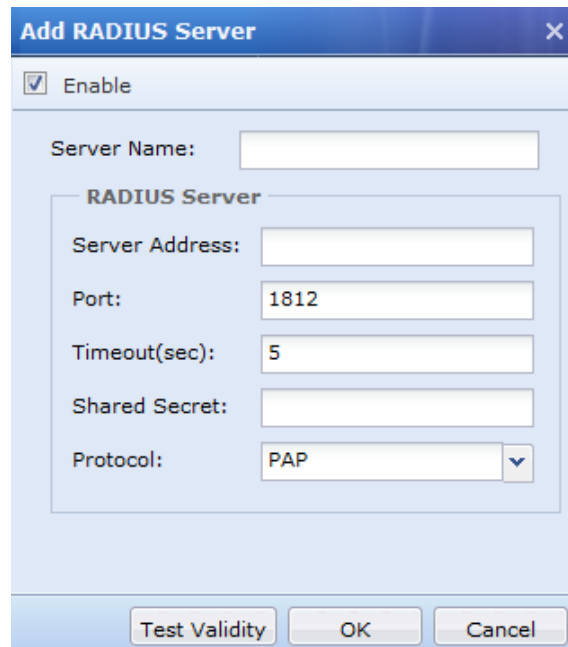
Test Effectiveness is used to verify the IP address, port number, and user name used for connecting the server.



In normal cases, retain the default value in the Search area.

Adding a RADIUS Server

Choose **User and Policy Management** on the navigation page. Choose **User Authentication** > **External Auth Server**. On the **External Auth Server** page, click **Add** and choose **RADIUS Server**. The **External Authentication Server (RADIUS)** page appears.



Add RADIUS Server [X]

☒ Enable

Server Name:

RADIUS Server

Server Address:

Port:

Timeout(sec):

Shared Secret:

Protocol: [v]

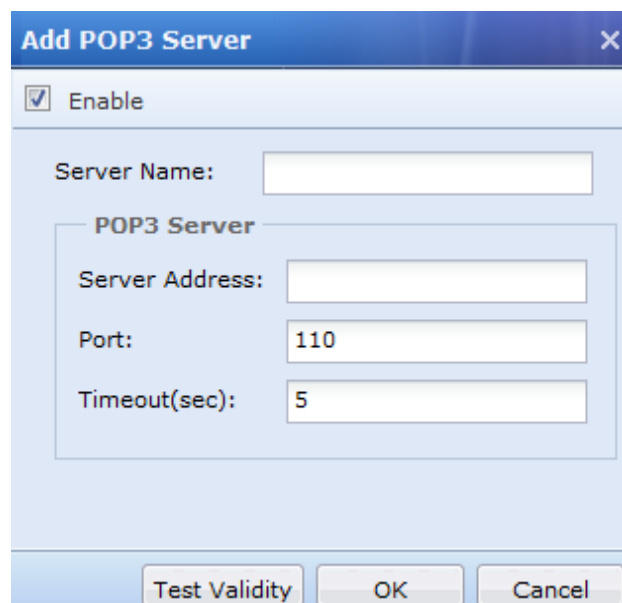
Test Validity OK Cancel

Enter a server name.

The **RADIUS Server** area is used to set the IP address, port number, timeout interval, shared secret, and protocol of the RADIUS server.

Adding a POP3 Server

Choose **User and Policy Management** on the navigation page. Choose **User Authentication** > **External Auth Server**. On the **External Auth Server** page, click **Add** and choose **POP3 Server**. The **External Auth Server (POP3)** page appears.



Add POP3 Server [X]

☒ Enable

Server Name:

POP3 Server

Server Address:

Port:

Timeout(sec):

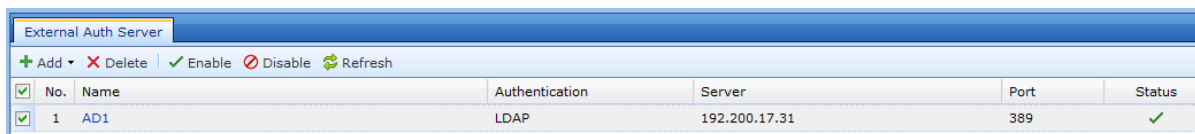
Test Validity OK Cancel

Enter a server name.

The **POP3 Server** area is used to set the IP address, port number, and timeout interval of the POP3 server.

Deleting an External Authentication Server

Step 1 Choose **User and Policy Management** on the navigation page. Choose **User Authentication > External Auth Server**. On the **External Auth Server** page, select the server to be deleted.

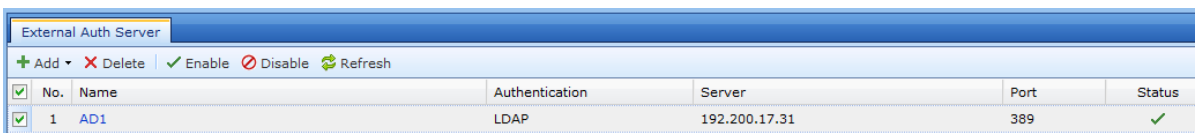


External Auth Server						
+ Add - Delete ✓ Enable ✗ Disable ↻ Refresh						
<input checked="" type="checkbox"/>	No.	Name	Authentication	Server	Port	Status
<input checked="" type="checkbox"/>	1	AD1	LDAP	192.200.17.31	389	✓

Step 2 Click **Delete**.

3.7.2.4.1 Enabling/Disabling an External Authentication Server

Step 1 Choose **User and Policy Management** on the navigation page. Choose **User Authentication > External Auth Server**. On the **External Auth Server** page, select the server to be enabled/disabled.



External Auth Server						
+ Add - Delete ✓ Enable ✗ Disable ↻ Refresh						
<input checked="" type="checkbox"/>	No.	Name	Authentication	Server	Port	Status
<input checked="" type="checkbox"/>	1	AD1	LDAP	192.200.17.31	389	✓

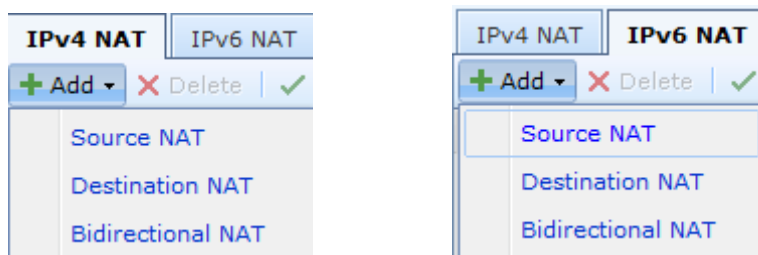
Step 2 Click **Enable/Disable**.

Firewall

The firewall module is used to set NAT, concurrent connection control rules, DoS/DDoS protection, and ARP protection. NAT includes source NAT, destination NAT, and bidirectional NAT. Through source NAT configuration, you can set rules to enable intranet users to access the Internet and set SNAT rules to implement other types of source address translation. Through destination NAT configuration, you can publish intranet servers on public networks and set DNAT rules to implement destination address translation.

NAT

The NGAF 5.2 supports IPv6 NAT feature. On the **NAT** page, click **IPv4 NAT** to configure for IPv4 environment and **IPv6 NAT** for IPv6 environment. Click on **Add** to select options for **Source NAT**, **Destination NAT** and **Bidirectional NAT** in both environment.



Source NAT

Source NAT translates source IP addresses of data that meet criteria. It is most commonly used when the device is deployed on the egress of the public network and intranet users need to access the public network. On the **IPv4 NAT** and **IPv6 NAT** page, you can manage, add, and delete source NAT rules.

Figure below shows **IPv4 Add Source NAT Rule** page :

Add Source NAT Rule

☒ Enable

Name: Access Internet

Description:

Source

Zone: InternalZonetest

IP Group: All

Destination

Zone/Interface: ☒ Zone
External-UKM

☐ Interface
eth0

IP Group: All

Protocol

Configure protocol and port Settings

Source Translation

To: Egress interface

Save and Add Another OK Cancel

Protocol and port settings are not available in IPv6 Source NAT. The figure below shows **Add IPv6 SNAT Rule**:

Add IPv6 SNAT Rule

☒ Enable

Name:

Description:

Source

Zone:

Subnet/Prefix: /

Destination

Zone:

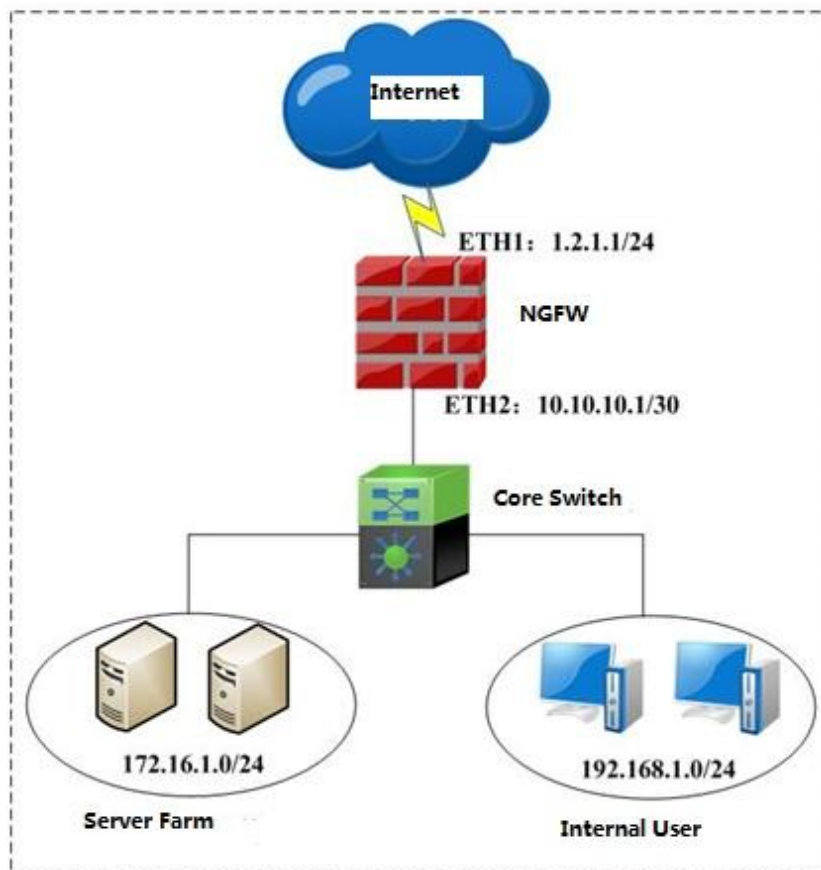
Source Translation

Translate Src To: /

Save and Add OK Cancel

3.8.1.1.1 Source NAT Configuration Example

A customer has the topology shown in the following figure. The intranet users and server groups of the customer require network access through the NGAF firewall. In this case, source NAT rules must be added on the NGAF device to change, when the data is transferred through the NGAF device, the IP addresses (192.168.1.0/24 and 172.16.1.0/24) of network access data to 1.2.1.1, which is the IP address of the ETH1 egress interface of the NGAF device.



Step 1 Before setting the source NAT rules, choose **Network Configuration > Interface/Zone**, click the **Zone** tab, define the home zone of the interface, and then choose **Object Definition > IP Group** and define the home IP group of the intranet segments. For configuration details, see sections 3.2.1.4 and 3.4.8. In this example, interface ETH1 is defined as an Internet zone and ETH2 is defined as an Intranet zone. 172.16.1.0/24 and 192.168.1.0/24 are defined as IP groups on the intranet. See the following figure:

Interfaces

Physical InterfaceSub-InterfaceVLAN InterfaceAggregate InterfaceZoneLink State Propagation

+ Add X Delete Refresh

<input type="checkbox"/>	Zone Name	Zone Type	Interfaces	Device Mgt Privilege	Allowed Address	Delete
-	LAN	Route(layer 3)	eth2	WebUI,snmp	All	In use
-	WAN	Route(layer 3)	eth1	WebUI,snmp	All	In use

IP Group

+ Add X Delete Refresh Import Export

<input type="checkbox"/>	No.	Name	Description	Delete
-	1	All	All IP addresses	In use
-	2	LAN IP Range		In use

Step 2 Click **Add** on the NAT page and choose **Source NAT**. The **Add Source NAT Rule** page shown in the following figure appears. Select **Enable** and enter a rule name and description. If you do not select **Enable**, the rule does not take effect. See the following figure:



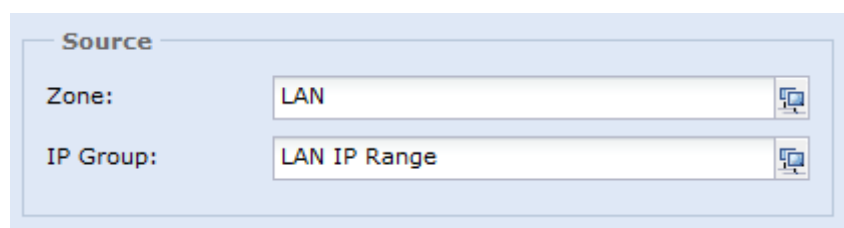
Add Source NAT Rule

☒ Enable

Name:

Description:

Step 3 Set **Zone** and **IP Group** to specify the IP addresses used for source NAT. Source NAT is implemented according to the rule only the data is from the specified IP addresses in the specified zone. If Internet access of the intranet is provided through a router interface, set the zone to the intranet and the IP group to intranet segments, or all network segments. In this example, **Zone** is set to **LAN** and **IP Group** is set to **LAN IP Range**. See the following figure:

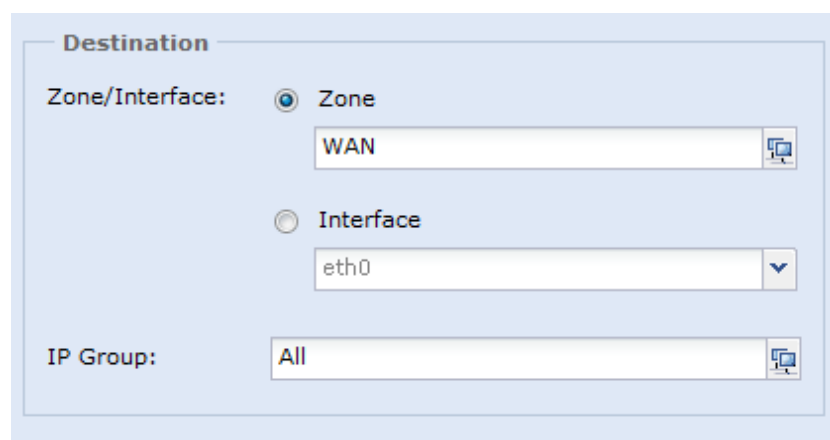


Source

Zone:

IP Group:

Step 4 Set Zone/Interface and IP Group in the Destination area to specify the destination zones and IP groups or interfaces to which the rule is applicable. If Internet access of the intranet is provided through a router interface, set the zone to the Internet and the IP group to all IP groups. In this example, **Zone** is set to **WAN** and **IP Group** is set to **All**. See the following figure:



Destination

Zone/Interface: ☒ Zone

☐ Interface

IP Group:

Step 5 Set the protocol. After you specify the protocol for source NAT, source NAT is implemented only for the data transferred through the destination and source interfaces that adopt the protocol. Click **OK**. In this example, the default values are retained.

Protocol and Port

Type:

Protocol No.:

Src Port: ☒ All ☐ Specified Port

Dst Port: ☒ All ☐ Specified Port

OK Cancel

Step 6 Set the parameters in the Source NAT area to specify the IP address to which the source IP address is changed when conditions including the source address, destination address, and protocol of data meet requirements. You can select **Egress interface**, **IP Range**, **IP Address**, or **Unchanged**. In this case, **Egress interface** is selected.

Source NAT

To:

- Egress interface
- IP Range
- IP Address
- IP Group
- Unchanged

Save and Add Another Cancel

Click **Save** to complete the source NAT rule configuration. See the following figure:

NAT

NATDNS Mapping

+ Add

✖ Delete

✓ Enable

✗ Disable

↑ Move Up

↓ Move Down

↔ Move

📁 Import

📁 Export




🔄 Refresh

Type: All

Original Data Packet																Translated Data Packet				
No.	Name	Type	Source...	Dst Zone/Int...	Source IP	Dst IP	Protocol	Src Port	Dst Port	Source IP	Dst IP	Dst Port	Hit C...	Status	Clone	Delete				
1	Internet acc...	SNAT	LAN	WAN	LAN IP Ra...	All	All	All	All	Egress int...	-	Unchanged	0	✓						

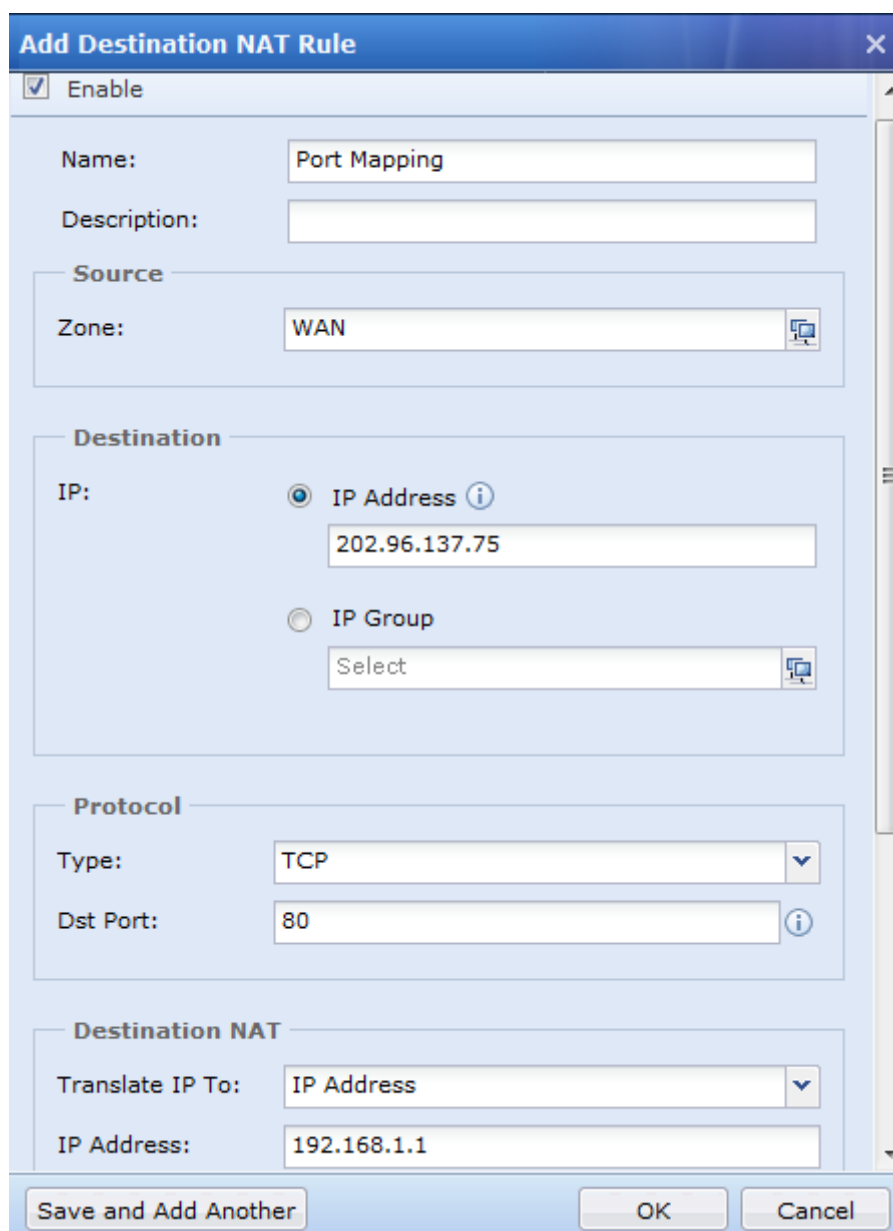


- To modify a source NAT rule, click the name of the rule to go to the modification page.
- To delete a source NAT rule, select the rule and click Delete, or click and follow the instruction to complete deletion.

- To disable a source NAT rule, click . When the rule is disabled, the status icon is changed to . To enable the rule again, click  and follow the instruction to enable the rule.
- You can add an IP group either by defining an object or when you select source NAT rules.

Destination NAT

Destination NAT changes the destination IP addresses of data transferred through the device. This is often used in mapping services on internal servers to the Internet so that Internet users can access the server. Click **Add** on the **IPv4 NAT** page, choose **Destination NAT**. The page shown in the following figure appears.



Add Destination NAT Rule

☒ Enable

Name: Port Mapping

Description:

Source

Zone: WAN

Destination

IP: ☒ IP Address 202.96.137.75 ☐ IP Group Select

Protocol

Type: TCP

Dst Port: 80

Destination NAT

Translate IP To: IP Address

IP Address: 192.168.1.1

Save and Add Another OK Cancel

Protocol and port settings are not available for IPv6 DNAT. Click on **Destination NAT** on **IPv6 NAT** page, the page in figure below will appear.


Add IPv6 DNAT Rule

☒ Enable

Name:

Description:

Source

Zone: 

Destination

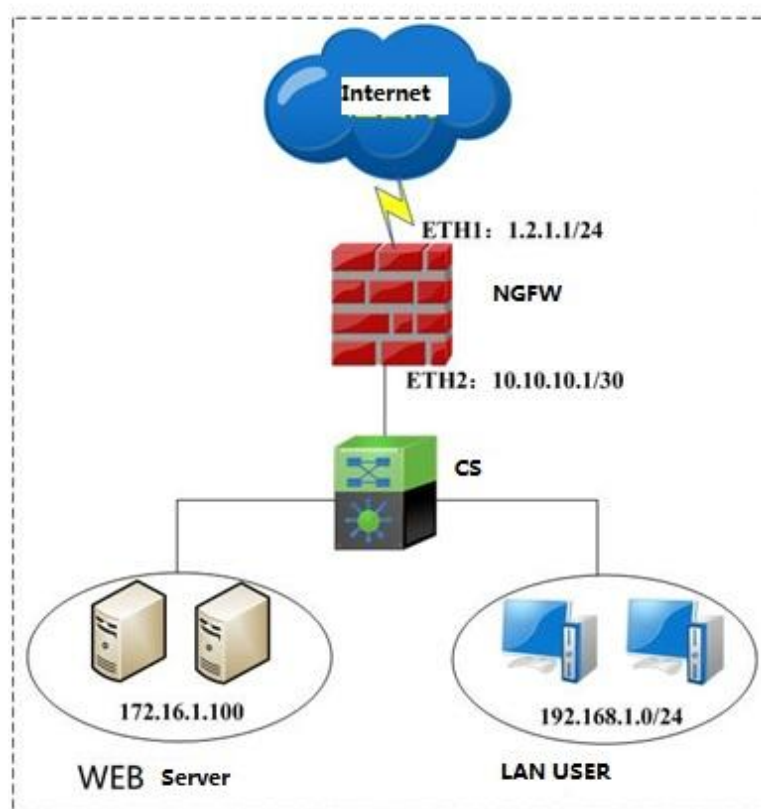
Subnet/Prefix: /

Destination Translation

Translate Dst To: /

3.8.1.2.1 Destination NAT Configuration Example

A customer has the topology shown in the following figure. There is a web server whose IP address and service port number are 172.16.1.100 and 80 on the intranet of the customer. The customer requires that Internet users can access the server by accessing <http://1.2.1.1>. This requirement can be met by destination NAT.



Step 1 Before setting the destination NAT rules, choose **Network > Interface/Zone**, click the **Zone** tab, define the home zone of the interface. For configuration details, see sections 3.2.1.4 and 3.4.8. In this example, interface ETH1 is defined as an Internet zone and ETH2 is defined as an Intranet zone. See the following figure:

Interfaces					
Physical Interface Sub-Interface VLAN Interface Aggregate Interface Zone Link State Propagation					
+ Add - Delete Refresh					
<input type="checkbox"/>	Zone Name	Zone Type	Interfaces	Device Mgt Privilege	Allowed Address
<input checked="" type="checkbox"/>	LAN	Route(layer 3)	eth2	WebUI,snmp	All
<input checked="" type="checkbox"/>	WAN	Route(layer 3)	eth1	WebUI,snmp	All

Step 2 Click **Add** on the NAT page and choose **Destination NAT**. The **Add Destination NAT Rule** page shown in the following figure appears. Select **Enable** and enter a rule name and description. If you do not select **Enable**, the rule does not take effect. See the following figure:

☒ **Enable**

Name:

Description:

Step 3 Specify the source zone of data whose destination IP addresses are to be changed. For example, if internal servers are published on the Internet, Internet users can access the server. In this example, **Zone** is set to **WAN**. See the following figure:

Source

Zone:

Step 4 Set **IP Address** or **IP Group** in the **Destination** area to specify the address for destination NAT when Internet users access the address. This IP address is the one accessed by users before destination NAT. Usually, it is the WAN IP address of an interface of the device. In this example, **IP Address** is set to **1.2.1.1**. See the following figure:

Destination

IP: ☒ **IP Address** i

☐ **IP Group**
 i

Step 5 Set the protocol and destination port number for destination NAT. In this example, the TCP protocol is used because the port number 80 for the HTTP service matches the TCP protocol. Set the destination port number to **80**. See the following figure:

Protocol

Type: v

Dst Port: i

Step 6 Set the destination IP address to which the original IP address is changed and specify whether the destination port number must be changed. In this example, the IP address of the internal server providing services through port number 80 based on the TCP protocol is 172.16.1.100, and the port number does not need to be changed. See the following figure:

Destination NAT

Translate IP To: v

IP Address:

Translate Port To: ☒ **Unchanged**
☐ **Specified Port**

Step 7 Click **Save** to complete the configuration. See the following figure:

NAT														
NAT DNS Mapping														
+ Add - Delete + Enable - Disable + Move Up - Move Down Move Import Export Refresh Type: All														
	No.	Name	Type	Sour...	Dst Zone/Int...	Original Data Packet				Translated Data Packet				
						Source IP	Dst IP	Protocol	Src Port	Dst Port	Source IP	Dst IP	Dst Port	Hit C...
	1	Web Server Publish Web...	DNAT	WAN	-	All 0.0.0.0-2...	1.2.1.1	TCP	All	80	-	172.16.1...	Unchanged	0
														Status Clone Delete

Step 8 Set application control policies to enable data to be transferred to the IP address 172.16.1.100 with the HTTP port number 80 from the Internet. For detailed configuration, see section 3.8.1.



- If the IP address 1.2.1.1 and port number 80 must be mapped to the IP address 172.16.1.100 and port number 8080 of the internal server, set Translate Port To to Specified Port and enter 8080. See the following figure:

Destination NAT

Translate IP To: IP Address

IP Address: 172.16.1.100

Translate Port To:

☐ Unchanged

☒ Specified Port

 8080

- To modify a destination NAT rule, click the name of the rule to go to the modification page.
- To delete a destination NAT rule, select the rule and click Delete, or click and follow the instructions to complete deletion.
- To disable a destination NAT rule, click . When the rule is disabled, the status icon is changed to . To enable the rule again, click and follow the instructions to enable the rule.

Bidirectional NAT

Bidirectional NAT means that one NAT rule involves translation of both source and destination IP addresses. The source and destination IP addresses of the data matching the rule are changed. This is usually used when intranet users access internal servers through public IP addresses or domain names. See the following figure:


Add Bidirectional NAT Rule


☒ Enable

Name:


Description:


Source


Zone: 


IP Group: 

Destination

Zone/Interface: ☒ Zone 

☐ Interface 

IP: ☒ IP Address 

☐ IP Group 

IPv6 Bidirectional NAT does not support protocol and NAT rule settings. Click on the **ADD -> Bidirectional NAT**, the page in figure below will appear.

Add IPv6 Bidirectional NAT Rule

☒ Enable

Name:

Description:

Source

Zone:

Subnet/Prefix: /

Destination

Zone:

Subnet/Prefix: /

Source Translation

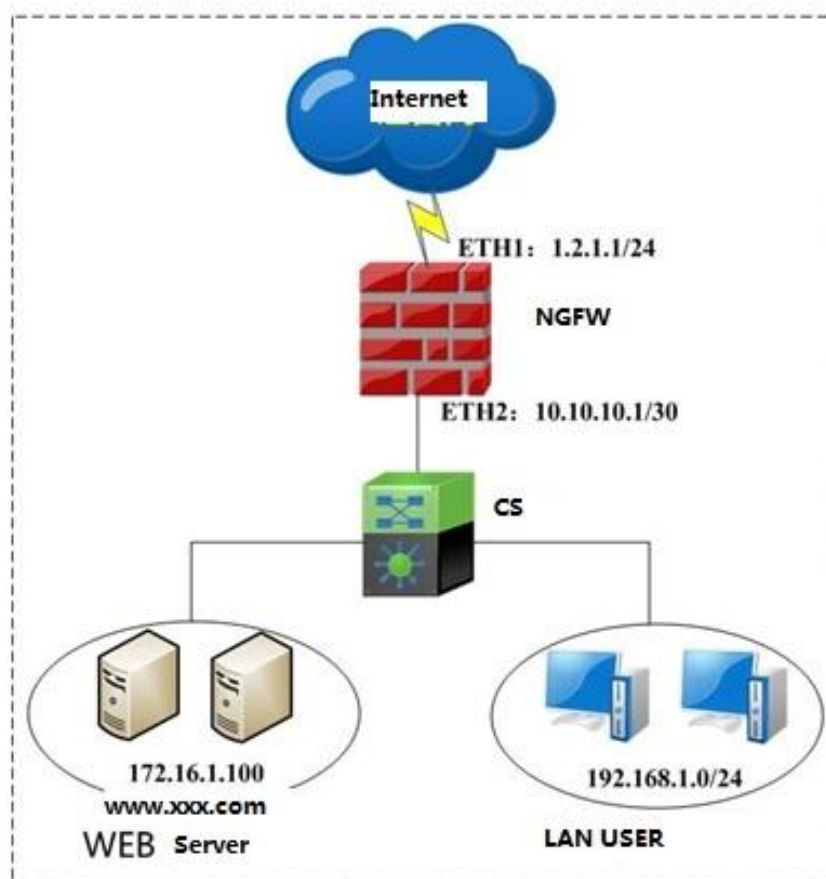
Translate Src To: /

Destination Translation

Translate Dst To: /

3.8.1.3.1 Bidirectional NAT Configuration Example

A customer has the topology shown in the following figure. There is an internal web server whose IP address is 172.16.1.100. The customer has applied for the domain name www.xxx.com and it points to 1.2.1.1. Currently, destination NAT has enabled Internet users to access the web server through www.xxx.com. However, the intranet users with 192.168.1.0/24 cannot access the server through the domain name. In this case, bidirectional NAT is required to enable the intranet users to access the web server with the domain name.



Step 1 Before setting the bidirectional NAT rules, choose **Network > Interface/Zone**, click the **Zone** tab, define the home zone of the interface, and then choose **Object > IP Group** and define the home IP group of the WAN interface. For configuration details, see sections 3.2.1.4 and 3.4.8. In this example, **ETH2** is set to **LAN**. 192.168.1.0/24 is defined as IP groups on the intranet. See the following figure:

Interfaces						
Physical Interface Sub-Interface VLAN Interface Aggregate Interface Zone Link State Propagation						
+ Add - Delete Refresh						
<input type="checkbox"/>	Zone Name	Zone Type	Interfaces	Device Mgt Privilege	Allowed Address	Delete
-	LAN	Route(layer 3)	eth2	WebUI,snmp	All	In use
-	WAN	Route(layer 3)	eth1	WebUI,snmp	All	In use

IP Group				
+ Add - Delete Refresh Import Export				
<input type="checkbox"/>	No.	Name	Description	Delete
-	1	All	All IP addresses	In use
-	2	LAN IP Range		In use

Step 2 Click **Add** on the NAT page and choose **Bidirectional NAT**. The **Add Bidirectional NAT Rule** page shown in the following figure appears. Select **Enable** and enter a rule name and description. If you do not select **Enable**, the rule does not take effect. See the following figure:



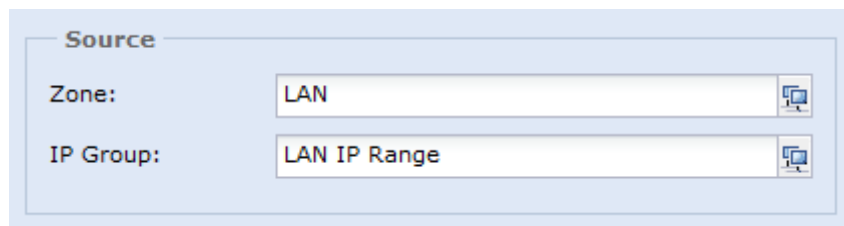
Add Bidirectional NAT Rule

☒ Enable

Name:

Description:

Step 3 Specify the source zone and source IP group to which the rule is applicable. In this example, the configuration is shown in the following figure.

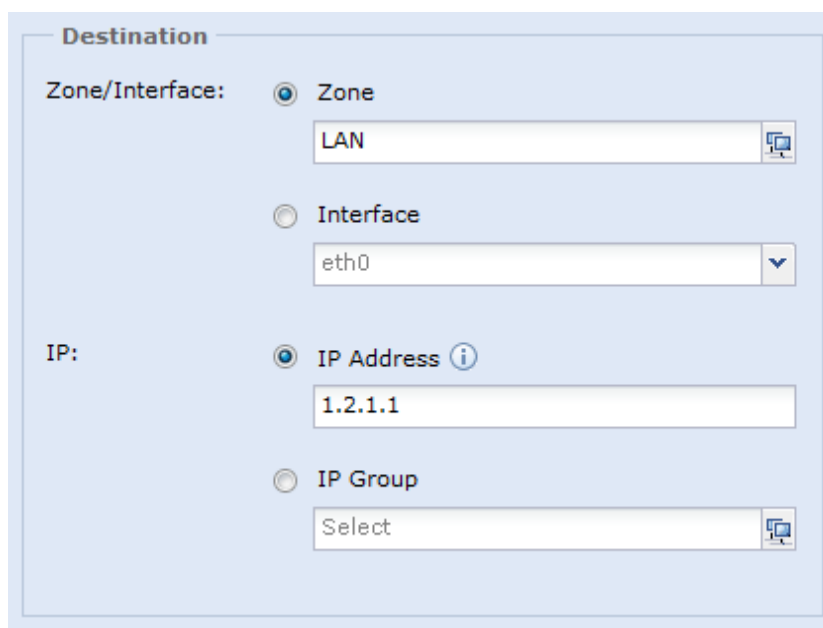


Source

Zone:

IP Group:

Step 4 Specify the destination IP address and destination zone to which the rule is applicable. In this example, the server is on the intranet and data must be sent from the intranet. Therefore, set **Zone** to **LAN**. The users access the server through the public address 1.2.1.1 of the device. Therefore, select **IP Address** and enter **1.2.1.1**. See the following figure:



Destination

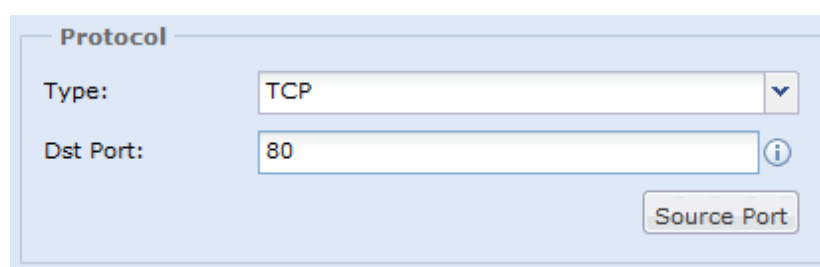
Zone/Interface: ☒ Zone

☐ Interface

IP: ☒ IP Address

☐ IP Group

Step 5 Set the protocol. In this example, access data is transferred from any source port number to the TCP 80 port number matching the IP address 1.2.1.1 for translation. See the following figure:

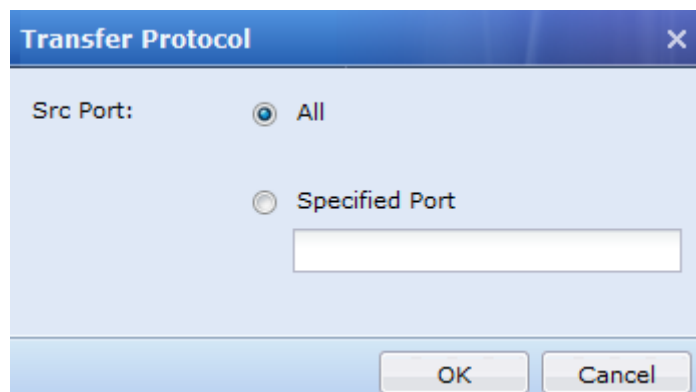


Protocol

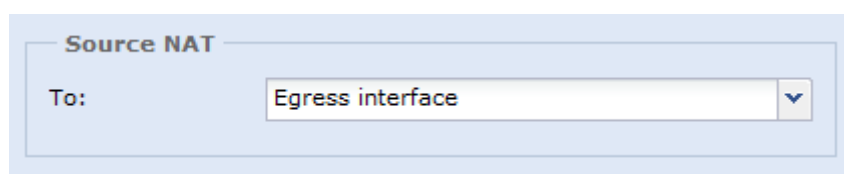
Type:

Dst Port:

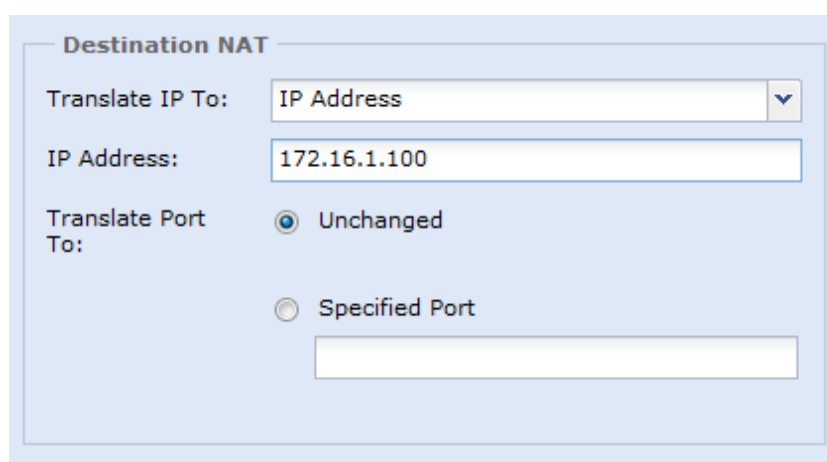
To restrict source port numbers of data packets, set **Src Port** to **Specified Port**. In this example, **Src Port** is set to **All**. See the following figure:

A dialog box titled "Transfer Protocol" with a close button (X) in the top right corner. It contains a "Src Port:" label followed by two radio button options: "All" (which is selected) and "Specified Port". Below the "Specified Port" option is an empty text input field. At the bottom right are "OK" and "Cancel" buttons.

Step 6 Set the source IP address to which the original source IP address is changed. In this example, it is set to the ETH2 intranet interface, which is the egress interface. See the following figure:

A configuration section titled "Source NAT". It contains a "To:" label followed by a dropdown menu showing "Egress interface" with a downward arrow icon.

Step 7 Set the destination IP address and port number to which the original destination IP address and port number are changed. In this example, the IP address 1.2.1.1 accessed by the users are changed to the IP address 172.16.1.100 of the intranet server, which the port number being unchanged. See the following figure:





A configuration section titled "Destination NAT". It contains a "Translate IP To:" label followed by a dropdown menu showing "IP Address". Below this is an "IP Address:" label followed by a text input field containing "172.16.1.100". Below that is a "Translate Port To:" label followed by two radio button options: "Unchanged" (which is selected) and "Specified Port". Below the "Specified Port" option is an empty text input field.

Step 8 Click **Save** to complete the bidirectional NAT rule configuration.

Step 9 Set application control policies to enable data to be transferred to the intranet IP address 172.16.1.100 with the HTTP port number 80 from the intranet. For detailed configuration, see section 3.8.1.



- You can add an IP group either by defining an object or when you select bidirectional NAT rules.
- To modify a bidirectional NAT rule, click the name of the rule to go to the modification page.

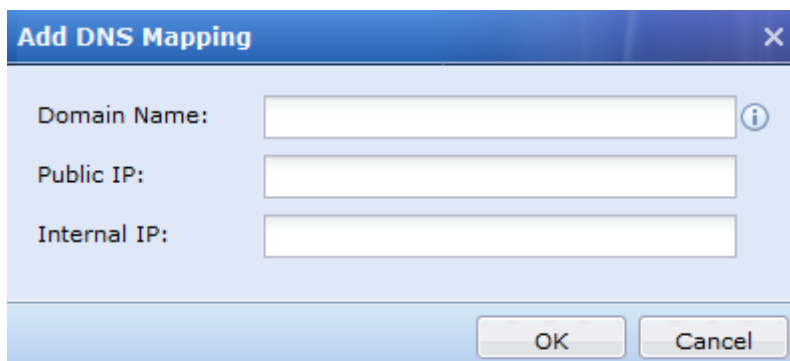
- To delete a bidirectional NAT rule, select the rule and click Delete, or click  and follow the instructions to complete deletion.
- To disable a bidirectional NAT rule, click . When the rule is disabled, the status icon is changed to . To enable the rule again, click  and follow the instructions to enable the rule.

DNS-Mapping

DNS Mapping is used to enable intranet users to access internal servers through public domain names. It implements the same function as bidirectional NAT. After DNS Mapping is set, the firewall resolves the domain name to the internal IP address of the server when an intranet user sends a DNS request. Then, the firewall sends the IP address to the user's client so that the client directly accesses the server without using NAT rules.

Differences between DNS Mapping and bidirectional NAT:

1. After DNS Mapping is set, server access data from the intranet is not transferred through the firewall. Instead, it is directly transferred to the IP address of the internal server. Bidirectional NAT transfers all data through the firewall. Therefore, DNS Mapping reduces workload of the firewall.
2. DNS Mapping can be set in an easier way than bidirectional NAT. It does not involve zones, IP groups, or port numbers. See the following figure:



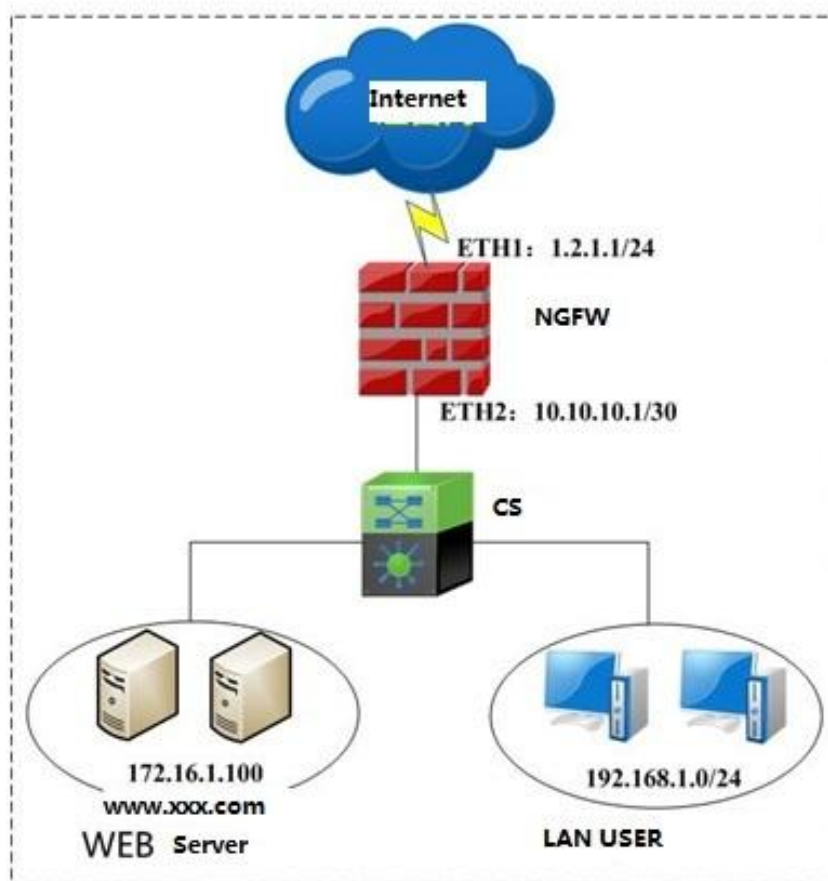
Domain Name: It specifies the domain name accessed by users.

Public IP: It specifies the public IP address corresponding to the domain name accessed by intranet users.

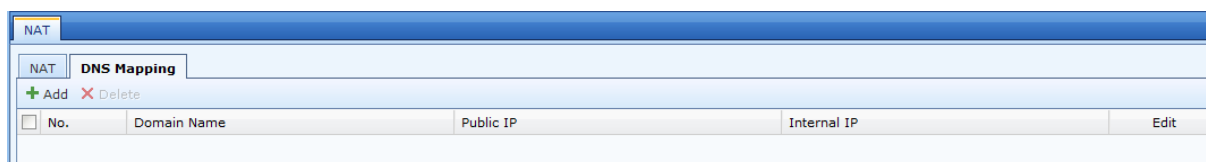
Internal IP: It specifies the internal IP address to be actually accessed.

3.8.1.4.1 DNS Mapping Configuration Example

A customer has the topology shown in the following figure. There is an internal web server whose IP address is 172.16.1.100. The customer has applied for the domain name www.xxx.com and it points to 1.2.1.1. The customer requires that intranet users (192.168.1.0/24) can access the server by accessing www.xxx.com. In this case, DNS Mapping can be used to enable the intranet users to access the web server through the domain name.



Step 1 Choose **NAT > DNA Mapping** and click **Add**.



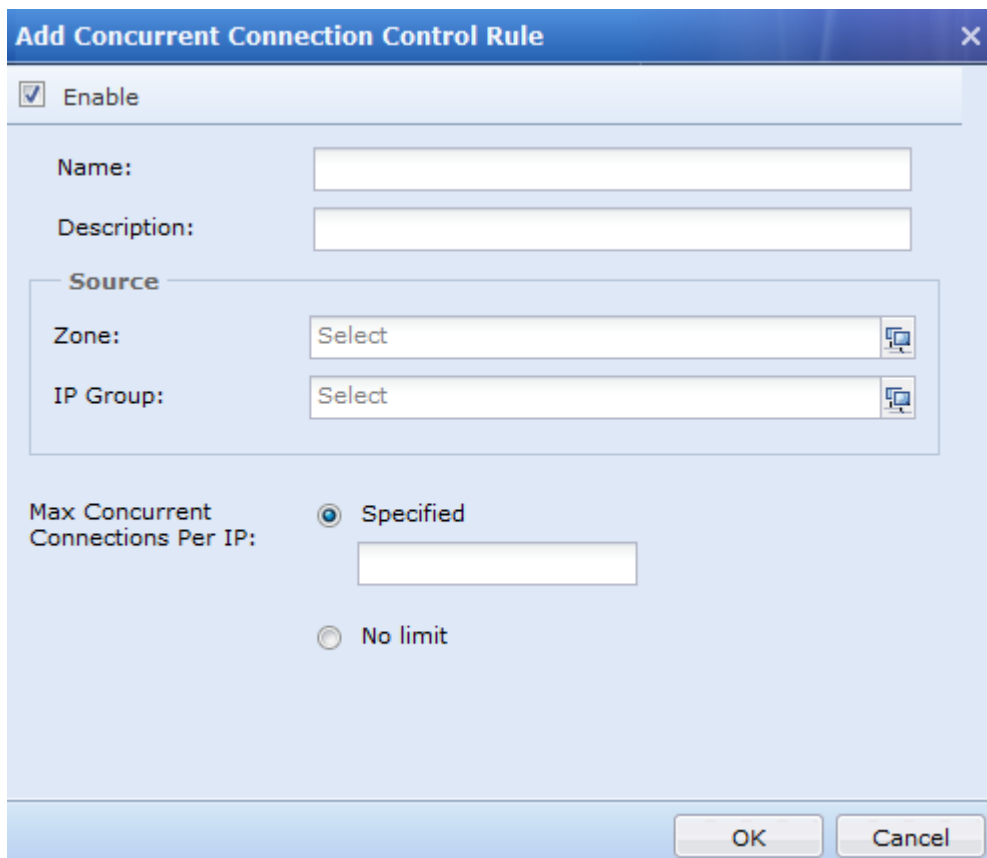
Step 2 Enter information such as the public IP address and domain name. The following figure shows the configuration for this example.

The 'Add DNS Mapping' dialog box contains three input fields: 'Domain Name' with the value 'www.xxx.com', 'Public IP' with the value '1.2.1.1', and 'Internal IP' with the value '172.16.1.100'. There is an information icon (i) next to the Domain Name field. At the bottom right are 'OK' and 'Cancel' buttons.

Step 3 Click **OK** to complete the configuration. The intranet users can directly access 172.16.1.100 by accessing www.xxx.com.

Concurrent Connections Control

Concurrent connections control is used to specify the maximum number of connections for each IP address. When an intranet user downloads content in P2P mode or a computer on the intranet is infected by a virus, there may be many connections set up in a short time. This affects device performance. In this case, you can set concurrent connections control to limit the maximum number of connections allowed for each IP address, which helps reduce network resource usage. See the following figure:



Name: It specifies the name of a rule. It can be customized.

Description: It specifies the description of a rule. It can be customized.

Zone: It specifies the zone where the maximum number of concurrent connections is limited. For details about how to set IP groups, see section 3.2.1.4.

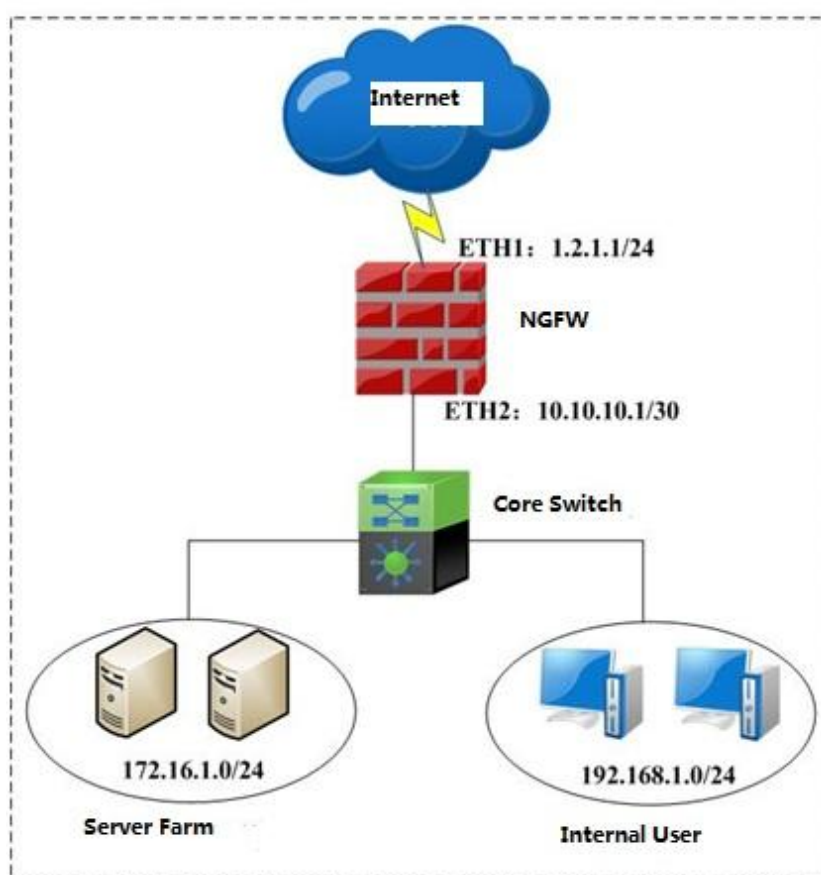
IP Group: It specifies the IP group for which the maximum number of concurrent connections is limited in a specified zone.

Max Concurrent Connections Per IP: It specifies the maximum number of concurrent connections allowed for each IP address.

1.1.1.1 Concurrent Connections Control Configuration Example

A customer has the topology shown in the following figure. The administrator requires that the concurrent connections of the intranet users in the 192.168.1.0/24 network segment are limited to 500 concurrent connections

per user.



Step 1 Before setting concurrent connections control, choose **Network > Interface/Zone**, click the **Zone** tab, define the home IP group of the WAN interface. For configuration details, see sections 3.2.1.4 and 3.4.8. In this example, ETH2 is defined as an Intranet zone and 192.168.1.0/24 is defined as an LAN IP group. See the following figure:

Interfaces					
Physical Interface	Sub-Interface	VLAN Interface	Aggregate Interface	Zone	Link State Propagation
+ Add X Delete Refresh					
<input type="checkbox"/>	Zone Name	Zone Type	Interfaces	Device Mgt Privilege	Allowed Address
<input checked="" type="checkbox"/>	LAN	Route(layer 3)	eth2	WebUI,snmp	All
<input checked="" type="checkbox"/>	WAN	Route(layer 3)	eth1	WebUI,snmp	All
					Delete
					In use
					In use

IP Group				
+ Add X Delete Refresh Import Export				
<input type="checkbox"/>	No.	Name	Description	Delete
<input checked="" type="checkbox"/>	1	All	All IP addresses	Delete
<input checked="" type="checkbox"/>	2	LAN IP Range		Delete
				In use
				In use

Step 2 On the concurrent connections control page, click **Add**. The **Add Concurrent Connection Control Rule** page appears. In this example, because the intranet users correspond to ETH2 and concurrent connections of the users must be limited, **Zone** is set to **LAN** and **IP Group** is set to **All**. See the following figure:

Add Concurrent Connection Control Rule

☒ Enable

Name:

Description:

Source

Zone:

IP Group:

Max Concurrent Connections Per IP:

☒ Specified

☐ No limit

OK Cancel

Step 3 Click **OK** to complete the configuration.



The number of TCP and UDP connections is limited as a whole.

DoS/DDoS Protection

DoS/DDoS attacks aim to terminate service responses by exhausting server resources. During such an attack, a great amount of fake request data is created to jam the server so as to prevent the server from responding to normal user requests. The SANGFOR device provides Internet and intranet protection against DoS attacks. This prevents intranets from being affected by DoS attacks from the internet and prevents computers on intranets infected with viruses or computers with attack tools on intranets from initiating DoS attacks.

Internet Protection

Choose **Firewall > DoS/DDoS Protection > Outside Attack**. The **Add Outside Attack Defense Policy** page appears. See the following figure:

Name: It specifies the name of a protection rule.

Description: It specifies the description of a protection rule.

Zone: It specifies the source zone to be protected. The source zone of Internet protection is usually an external zone.

Defense against ARP flooding attack: ARP flooding attack protection is enabled when this option button is selected. You can set **Per-Src-Zone packets Threshold** to specify the upper limit on ARP packets received by an interface in the specified zone per second. If the upper limit is exceeded, it is regarded as an attack. If **Deny** is selected as an action to be taken when being attacked, excessive ARP packets are discarded when an attack is detected.

IP scan prevention: IP scan prevention is enabled when this option button is selected. You can set **Threshold** to specify the upper limit on scan packets received from an IP address in the specified source zone per second. If the upper limit is exceeded, it is regarded as an attack. If **Deny** is selected as an action to be taken when being attacked, all data from the IP address is blocked within 5 minutes when an attack is detected. After 5 minutes, the number of scan packets from the IP address is recalculated.

Port scan prevention: Port scan prevention is enabled when this option button is selected. You can set **Threshold** to specify the upper limit on port scan packets received from an IP address in the specified source zone per second.

If the upper limit is exceeded, it is regarded as an attack. If **Deny** is selected as an action to be taken when being attacked, all data from the IP address is blocked within 5 minutes when an attack is detected. After 5 minutes, the number of port scan packets from the IP address is recalculated.

After the preceding treatment, data packets are filtered through Defense Against DoS/DDoS Attack, Packet-Based Attack, and Abnormal Message Probe.

Defense Against DoS/DDoS Attack: Select Select type. The page shown in the following figure appears.

Dst IP:

☐ **Defense against ICMP flooding attack**
Per-Dst-IP Packet Threshold (packets/sec):

☐ **Defense against UDP flooding attack**
Per-Dst-IP Packet Threshold (packets/sec):

☐ **Defense against SYN flooding attack**
Per-Dst-IP Packet Threshold (packets/sec):
Per-Dst-IP Packet Loss Threshold (packets/sec):
Per-Src-IP Packet Loss Threshold (packets/sec):

☐ **Defense against DNS flooding attack**
Per-Dst-IP Packet Threshold (packets/sec):

Dst IP: It specifies the destination server or server group to be protected. DoS/DDoS protection applies only to the data transferred from the Internet to the destination IP or IP group based on the following thresholds.

Defense against ICMP flooding attack: ICMP flooding attack protection is enabled when this option button is selected. You can set **Per-Dst-IP Packet Threshold** to specify the upper limit on the ICMP packets from the specified source zone to an IP address per second. If the upper limit is exceeded, it is regarded as an attack. If **Deny** is selected as an action to be taken when being attacked, excessive ICMP packets are discarded when an attack is detected.

Defense against UDP flooding attack: UDP flooding attack protection is enabled when this option button is selected. You can set **Per-Dst-IP Packet Threshold** to specify the upper limit on the UDP packets from the specified source zone to an IP address per second. If the upper limit is exceeded, it is regarded as an attack. If **Deny** is selected as an action to be taken when being attacked, excessive UDP packets are discarded when an attack is detected.

Defense against SYN flooding attack: SYN flooding attack protection is enabled when this option button is selected. When the number of SYN packets from the specified source zone to an IP address per second exceeds the upper limit specified by **Per-Dst-IP Packet Threshold**, the SYN proxy is activated to protect the intranet server.

When the number of SYN packets from the specified source zone to an IP address per second exceeds the upper limit specified by **Per-Dst-IP Packet Loss Threshold**, excessive SYN packets are discarded. When the number of SYN packets from an IP address in the specified source zone to a destination IP address or IP group per second exceeds the upper limit specified by **Per-Src-IP Packet Loss Threshold**, the source IP address is regarded as the attack source and excessive SYN packets are discarded.

Defense against DNS flooding attack: DNS flooding attack protection is enabled when this option button is selected. You can set **Per-Dst-IP Packet Threshold** to specify the upper limit on the DNS packets from the specified source zone to an IP address per second. If the upper limit is exceeded, it is regarded as an attack. If **Deny** is selected as an action to be taken when being attacked, all DNS packets sent to the IP address are discarded when an attack is detected.

After the configuration, click **OK** and continue setting other protection options shown in the following figure.

Defense Against DoS/DDoS Attack

Attack Type: [Selected: Defense against ICMP flooding ...](#)

Packet-Based Attack

Attacks: [Selected: Unknown protocol, TearDrop atta...](#)

Abnormal Message Probe

Bad IP Options : [Select type](#)

Bad TCP Options: [Select type](#)

Action

☒ Log event ☒ Deny

Defense Against DoS/DDoS Attack: Select **Select type**. The page shown in the following figure appears.

Packet-Based Attack

- ☐ Name
- ☒ Unknown protocol
- ☐ TearDrop attack
- ☐ IP packet splitting
- ☐ LAND attack
- ☐ WinNuke attack
- ☐ Smurf attack
- ☐ Huge ICMP pak attack(> 1024B)#Ping of death

OK Cancel

Unknown protocol: Protection against unknown protocol is enabled when this option button is selected. A protocol

with an ID greater than 137 is regarded as an unknown protocol.

TearDrop attack: TearDrop attack protection is enabled when this option button is selected. This protection is implemented by restricting fragment offset in an IP packet header. If fragment offset fails to meet requirements, it is regarded as a TearDrop attack.

IP packet splitting: IP packet splitting is not allowed when this option button is selected. If IP packet fragments are transferred, it is regarded as an attack.

LAND attack: LAND attack protection is enabled when this option button is selected. When the NGAF detects that the source and destination addresses of a data packet are the same, the packet is regarded as a LAND attack.

WinNuke attack: WinNuke attack protection is enabled when this option button is selected. If the URG flag of a TCP packet header is 1 and the destination port number is TCP139 or TCP445, the packet is regarded as a WinNuke attack.

Smurf attack: Smurf attack protection is enabled when this option button is selected. When the device detects that the response address of a packet, which is an ICMP response request packet, is a broadcast address, it is regarded as a Smurf attack.

Huge ICMP pak attack: If this option button is selected, it is regarded as an attack when an ICMP packet exceeds 1024 bytes.

After the configuration, click **OK** to save the configuration of packet-based attack protection. You can continue setting other Internet attack protection options shown in the following figure.

Packet-Based Attack

Attacks: [Selected: Unknown protocol, TearDrop attack...](#)

Abnormal Message Probe

Bad IP Options : [Select type](#)

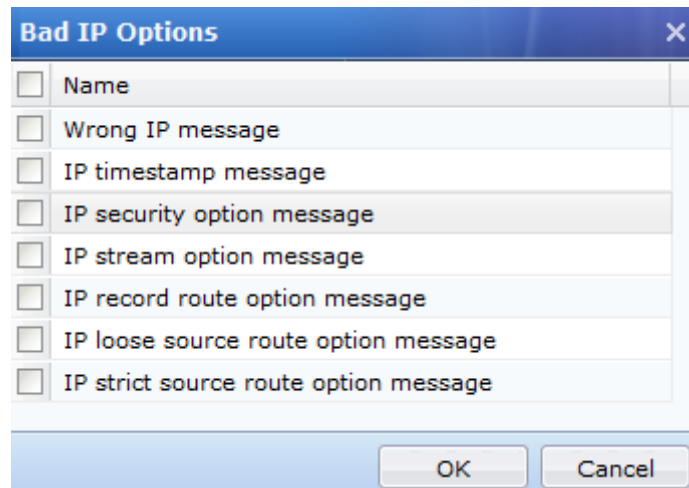
Bad TCP Options: [Select type](#)

Action

☒ Log event ☒ Deny

Abnormal Message Probe: It detects abnormal packets, mainly IP packets and TCP packets.

Bad IP Options: Select **Select type**. The page shown in the following figure appears.

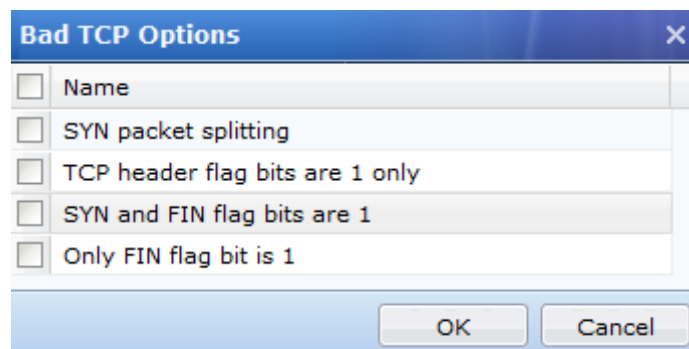


Bad IP options include **IP timestamp message**, **IP security option message**, **IP stream option message**, **IP record route option message**, **IP loose source root option message**, and **IP strict source root option message**. Normal IP packets do not contain these options. IP packets containing these options are usually used in attacks. To disallow IP packets to contain these options, select the corresponding check boxes.

To disallow IP packets to contain other options, select **Wrong IP message**.

Click **OK** to save the configuration.

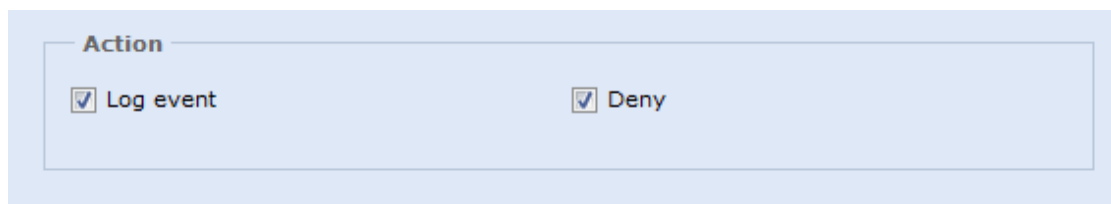
Bad TCP Options: Select **Select type**. The page shown in the following figure appears.



Bad TCP options include **SYN packet splitting**, **TCP header flag bits are 1 only**, **SYN and FIN flag bits are 1**, and **Only FIN flag bit is 1**. Normal TCP packets do not contain the options. Exception may occur when the destination server cannot properly process the TCP packets containing the options. To disallow TCP packets to contain the options, select the corresponding check boxes.

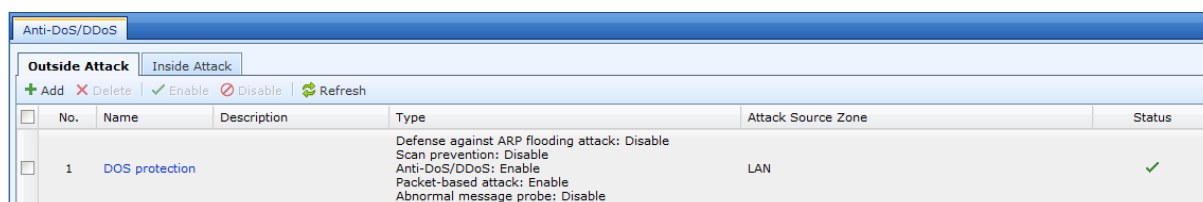
Click **OK** to save the configuration.

After setting the protection options, select the action to be taken when being attacked. See the following figure:



If **Log event** is select, logs are recorded when an attack is detected and the attack is not blocked. To block the attack when recording logs, select **Deny**.

Click **OK** to save the configuration.



Anti-DoS/DDoS						
Outside Attack			Inside Attack			
+ Add - Delete ✓ Enable ✗ Disable ↻ Refresh						
<input type="checkbox"/>	No.	Name	Description	Type	Attack Source Zone	Status
<input type="checkbox"/>	1	DOS protection		Defense against ARP flooding attack: Disable Scan prevention: Disable Anti-DoS/DDoS: Enable Packet-based attack: Enable Abnormal message probe: Disable	LAN	✓

You can click **Add** to add other Internet attack protection rules.

To modify an Internet attack protection rule, click the name of the rule. To delete a rule, select it and click **Delete**. To enable a rule, click **Enable**. To disable a rule, click **Disable**. To move a rule upward or downward, click **Up** or **Down**. Rule matching is implemented from top to bottom.



- **Matching between packets and rules is implemented from top to bottom of the rule list. If a packet is discarded according to a rule, the subsequent rules are not used. If a packet does not match a rule, the subsequent rule is used to check whether the packet represents an attack.**
- **If you have set scan protection, it is recommended that you set ICMP attack protection contained in DoS/DDoS attack protection as well. This mainly depends on attack characteristics. Usually, hackers scan IP addresses and then port numbers to find attack targets. After detecting IP addresses and port numbers, they will carry out next attack action. Some hackers know IP addresses and port numbers in advance so they can direct attack the targets. Therefore, both protection measures are recommended to ensure effective protection.**

Intranet Protection

Choose **Firewall > DoS/DDoS Protection > Inside Attack**. The **Inside Attack** page appears. See the following figure:

Source Zone: The source zone of intranet protection is usually an internal zone.

Source Address: It specifies the IP addresses from which packets can be transferred through the firewall. If **Only allow packets from the following sources** is selected, only the packets from the specified IP addresses can be transferred through the firewall. The other packets are discarded by the firewall.

Device Deployment: Directly connect to intranet through L2 switch, no L3 switch in between: This option is not recommended. If the device is directly connected to the intranet through an L2 switch without an L3 switch in between, you can select this option. But this option is not mandatory. By default, the device detects attacks based on IP addresses. If this option is selected, the device detects attacks based on MAC addresses. The reason why this option cannot be selected when the intranet has L3 switches is that the MAC addresses of data transferred through an L3 switch are changed to the MAC address of the L3 switch. This may cause the device to discard all Internet access data from the intranet.

IP Exclusion: DoS protection is not implemented for the IP addresses in the list. For example, if there is a server on the intranet that provides services for the Internet and sets up many connections with the Internet, it is recommended that the IP address of the server be added to the list. This prevents the IP address from being blocked by DoS protection.

Max TCP Connections: It specifies the maximum TCP connections that can be set up from an IP address within 1

minute to a port number of another IP address. If the upper limit is exceeded, the source IP address is locked for a specified period.

Max Attack Packets: It specifies the maximum number of attack packets (including SYN, ICMP, and TCP/UDP packets) that can be sent by a host within 1 second. If the upper limit is exceeded, the IP address or MAC address of the host is locked for a specified period.

Lockout Period (min): It specifies the period (in minutes) in which a host making an attack is locked after the device detects the attack.

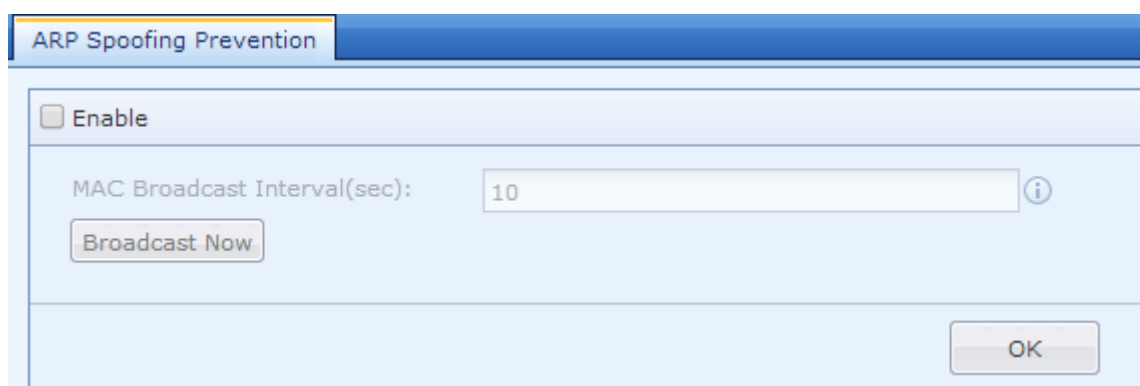
ARP Spoofing Protection

ARP spoofing is a common intranet virus. Computers infected by the virus irregularly send ARP spoofing broadcast packets on the intranet to disrupt normal communication between computers on the intranet. Sometimes it causes network breakdown.

The device protects its ARP cache by denying ARP requests or responses that carry attack characteristics.

If the access-controlled users of the device have bound IP addresses or MAC addresses, the device uses the IP addresses or MAC addresses for protection.

See the following figure:



Enable: The device regularly broadcast its MAC address if this option button is selected.

MAC Broadcast Interval (sec): It specifies the interval for broadcasting the MAC address of the device.

Access Control

Network insecurity usually results from unlimited insecure content access by intranet users. The SANGFOR NGAF device ensures Internet content security using application control policies, anti-virus policies, and anti-malware.

Application Control Policy

It filters Internet data based on application layer characteristics of packets or port numbers of packets. For example, it can prevent intranet users from playing games in work hours. Setting of this module requires the objects, including service, IP group, schedule, and application characteristic library, in **Object Settings**.

Choose **Access Control > Application Control Policy**. On the page that appears, you can add, delete, enable, disable, and search for application control policies. By default, the device has a policy for denying all services or applications. See the following figure:

Application Control Policy										
		+ Add X Delete		✓ Enable ✗ Disable		↑ Move Up ↓ Move Down		↔ Move	📁 Import	
		Source Zone: All		Dst Zone: All						
No.	Name	Source Zone	Source IP/User	Dst Zone	Dst IP	Service/Application	Schedule	Action	Log...	Hit Co...
1	all test	WAN LAN	All 0.0.0.0-255.255.2...	LAN WAN	All 0.0.0.0-255.255.2...	Predefined Service/any	All week	➡ Allow	No	47 ✓
- 2	Default Policy	All	All	All	All	All/All	All week	✗ Deny	No	0 ✓

Click **Add**. The **Add Application Control Policy** page appears. See the following figure:

Add Application Control Policy

☒ Enable

Name:

Description:

Source

IP/User:

☒ IP Group

Select

☐ User/Group

Select

Zone:

Select

Destination

IP Group:

All

Zone:

Select

Service/Application

Service/Application:

☒ Service

Select

☐ Application

Select

Save and Add Another

OK

Cancel

Enable: An application control policy is enabled when this option button is selected.

Name: It specifies the name of a policy.

Description: It specifies the description of a policy.

Source Zone: To control Internet access data of intranet users, set the source zone to an internal zone. **IP/User:** It specifies whether to control data based on source IP addresses or users. **User/Group:** It specifies the user

information invoked from **Authentication System > User Management > Group/User**.

Destination Zone: It specifies the destination zone of the data to be controlled. To control Internet access data of intranet users, set the destination zone to an external zone.

IP Group: It specifies the destination IP group of the data to be controlled. To control Internet access data of intranet users, set the destination IP group to **All**.

Service/Application: It specifies the service or application that requires data control. **Application** is the application characteristics invoked from **Object Definition > Application Characteristic Library**. **Service** is the service defined in **Object Definition > Service**.

Schedule: The policy takes effect only in the specified period. The values are defined in **Object Definition > Schedule**.

Action: It specifies whether the packets meeting the preceding criteria are discarded or not.

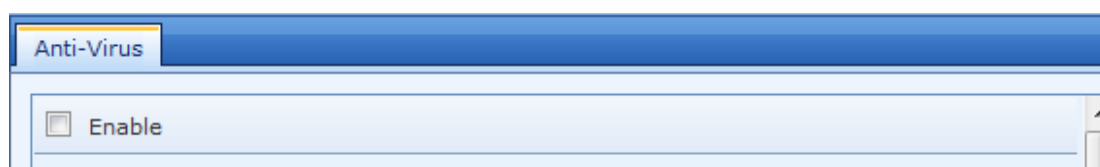
Log: Control actions are recorded in the embedded data center when this option button is selected.

Anti-Virus Policy

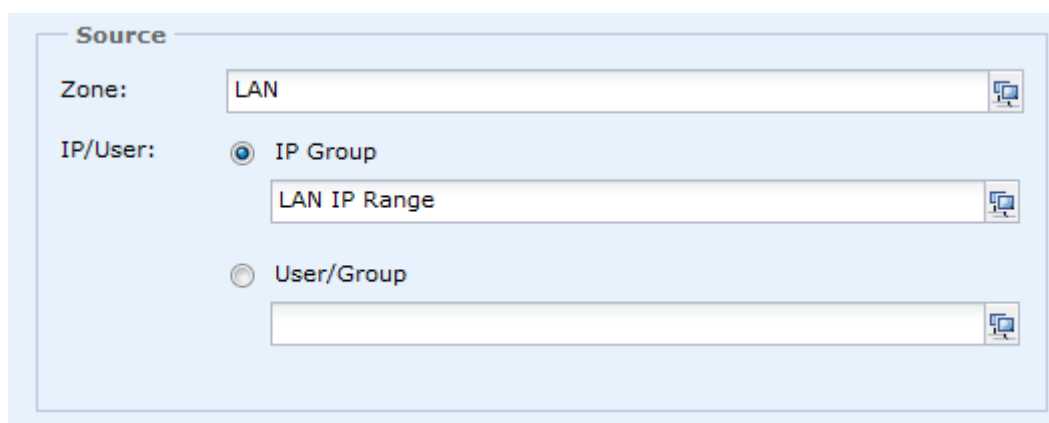
Anti-virus policies are used mainly to detect and remove viruses from data transferred through the device to protect data in specified zones. The device can detect and remove viruses based on the HTTP, FTP, POP3, and SMTP protocols. It is embedded with the anti-virus engine from the world's famous anti-virus software provider SOPHOS. The engine features high virus detection rate and high virus removal efficiency. The virus definition library of device is synchronized with SOPHOS's virus definition library once every one to two days.

Choose **Access Control > Anti-Virus Policy**. The **Anti-Virus** page appears. The device allows only one anti-virus policy, which is often used to prevent intranet users' computers from being infected by viruses. The configuration procedure is as follows:

Step 1 Select **Enable**.



Step 2 Set the source objects to be protected, such as all the users on the intranet. See the following figure:

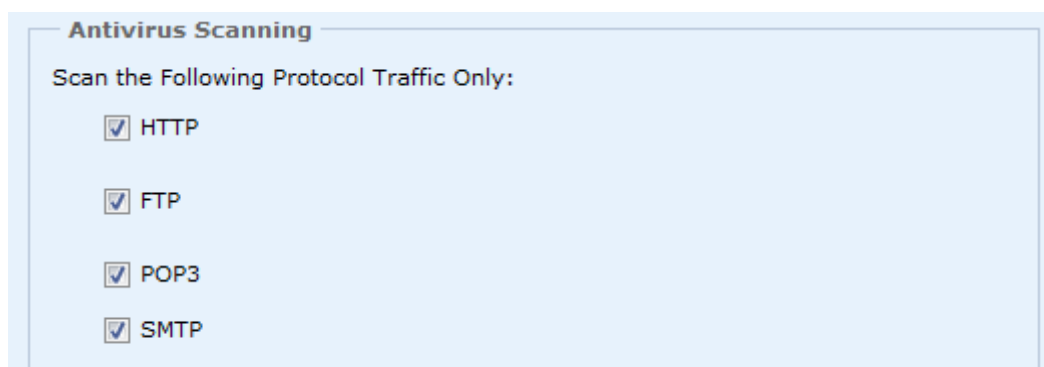


Step 3 Specify the destination zones to which anti-virus protection is implemented when users in source zones access the destination zones. For example, anti-virus protection is implemented for all IP addresses accessing the Internet. See the following figure:



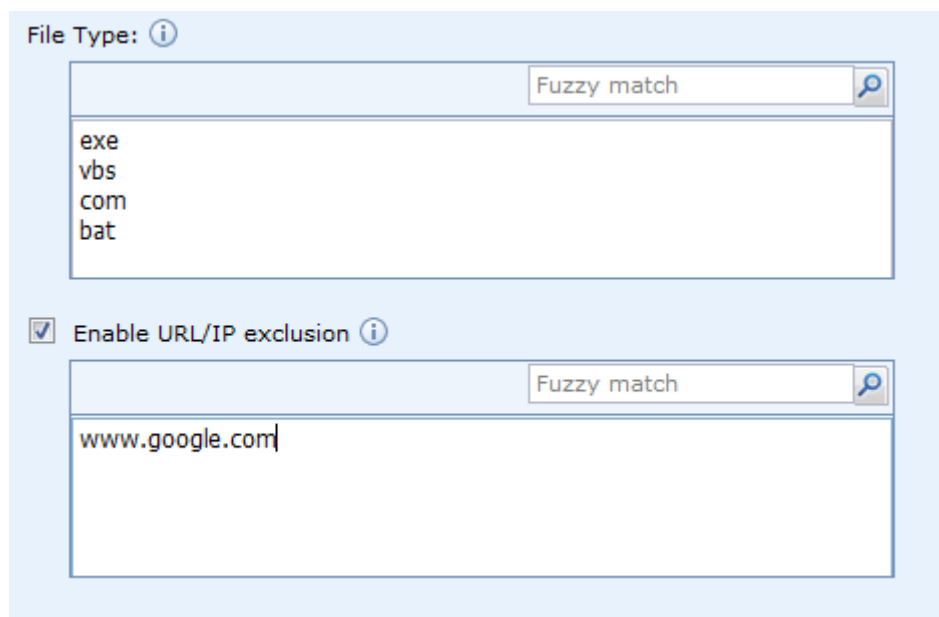
The 'Destination' configuration window contains two fields. The 'Zone:' field is set to 'WAN' and the 'Dst IP Group:' field is set to 'All'. Both fields have a small icon to their right.

Step 4 Specify the protocols (including HTTP, FTP, POP3 for sending emails, and SMTP for receiving emails) for which anti-virus protection is implemented. Select all the protocols. See the following figure:



The 'Antivirus Scanning' configuration window has a section titled 'Scan the Following Protocol Traffic Only:'. Below this title are four checkboxes, all of which are checked: HTTP, FTP, POP3, and SMTP.

Step 5 Set other supplementary options.



The configuration window for supplementary options is divided into two sections. The top section, 'File Type', has an information icon and a 'Fuzzy match' dropdown. Below it is a text area containing the file extensions: exe, vbs, com, and bat. The bottom section, 'Enable URL/IP exclusion', has a checked checkbox and an information icon. It also features a 'Fuzzy match' dropdown and a text area containing the URL: www.google.com.

File Type: It specifies the file types that require virus removal. The device removes viruses only for the files matching the file types in the list. This configuration is applicable only to HTTP and FTP applications.

Enable URL/IP exclusion: It excludes specified websites from anti-virus protection and is applicable only to HTTP. You can enter one domain name or IP address in each line. Wildcard is supported. Usually, anti-virus software providers' websites must be excluded so that the virus definition libraries of anti-virus software installed on computers on the intranet can be updated properly.

Action: It specifies the action to be taken when an attack is detected. The options include **Log Event** and **Deny**.

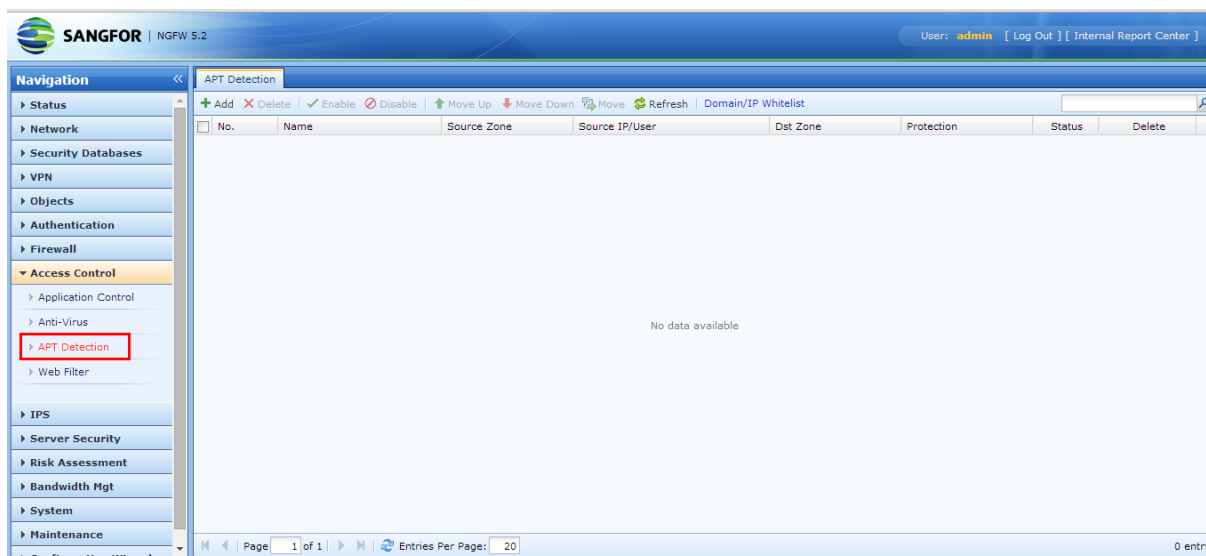
Click **OK** to complete the configuration.



The device removes viruses only for the files matching the file types specified.

APT Detection

If users have found and isolated computers on the intranet that are infected by viruses or Trojan horses, anti-malware protection enables the device to identify the traffic of the viruses or Trojan horses when they try to communicate with the Internet, block the traffic based on the users' policies, and record logs. See the following figure:



Choose **Access Control > APT Detection**. On the page that appears, you can add, delete, enable, and disable anti-malware policies. The following figure shows after user clicked on the **Add** button:

Add APT Detection Rule

☒ Enable

Name:

Description:

Protection

Zone:

IP/User: ☒ IP Group

☐ User/Group

Security Options

☒ Remote Access Trojan

☒ Malicious Connection(Cloud-Based Sandbox)

☒ Mobile Security(Cloud-Based Sandbox)

☒ Abnormal Traffic [Settings](#) ⓘ

Action

Action: ☒ Allow ☐ Deny ⓘ

IP Lockout: ☐ Affiliated Source Lockout

Logging: ☒ Log event

Name: Define name for the policy.

Description: Description for the policy

Protection

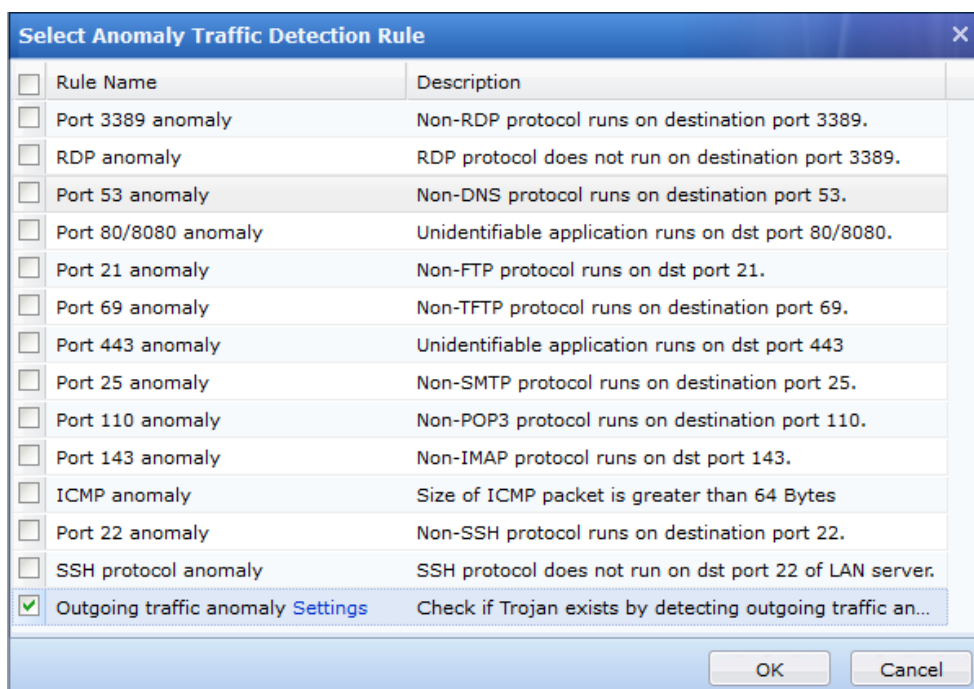
Zone: Select the zone where the policy will apply protection to.

IP/User: Select the protection IP and User for the policy.

Security Options

There available security protection options are **Remote Access Trojan, Malicious Link (Cloud-Based Sandbox), Mobile Security (Cloud-Based Sandbox)** and **Abnormal Connection**.

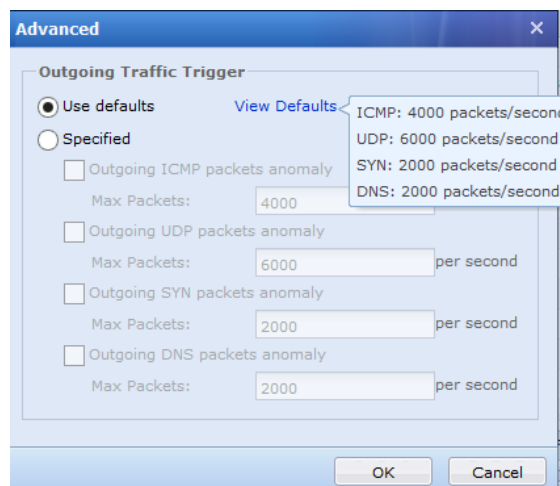
Click on the **Settings** on the right of **Abnormal Connection** and the page below is shown:



Select the related rule desired to protect from abnormally connection attacks.

Outgoing traffic anomaly is selected as default. Click **Settings** on the right of Outgoing traffic anomaly.

It will display **Advanced** for Outgoing traffic anomaly. See the figure below.




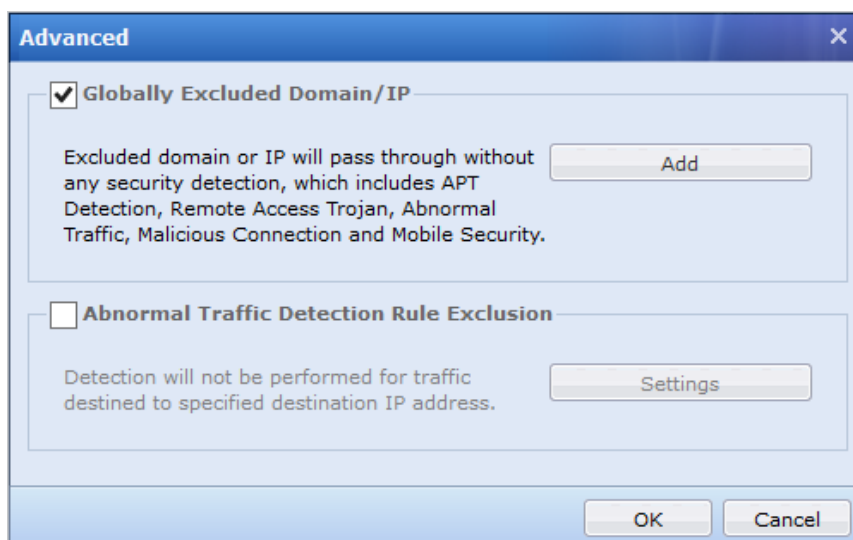
Action: Select to allow or deny the connection which hits the rule in this policy.

Logging: Check on the log event checkbox to record all the connections which match the policy rules.

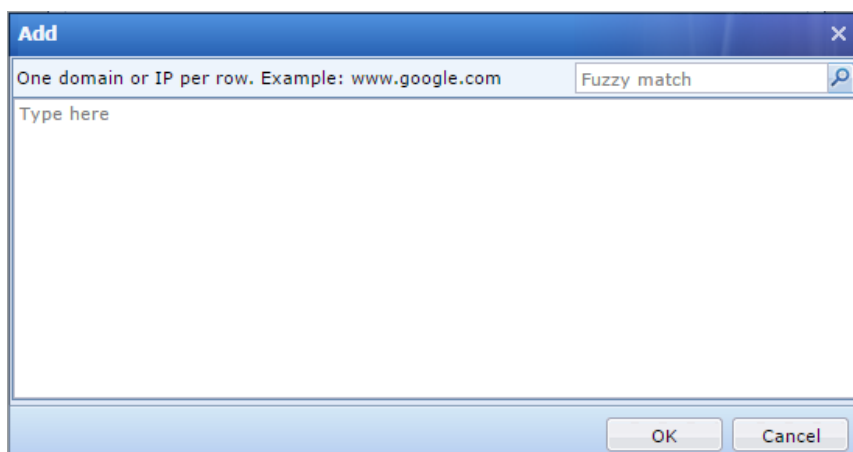


If policies have been set in Security Protection Objects and Zombie Network Rule Library, when packets matching the policies are transferred through the device, the packets are not denied though Action is set to Deny in Add Anti-Malware Rule.

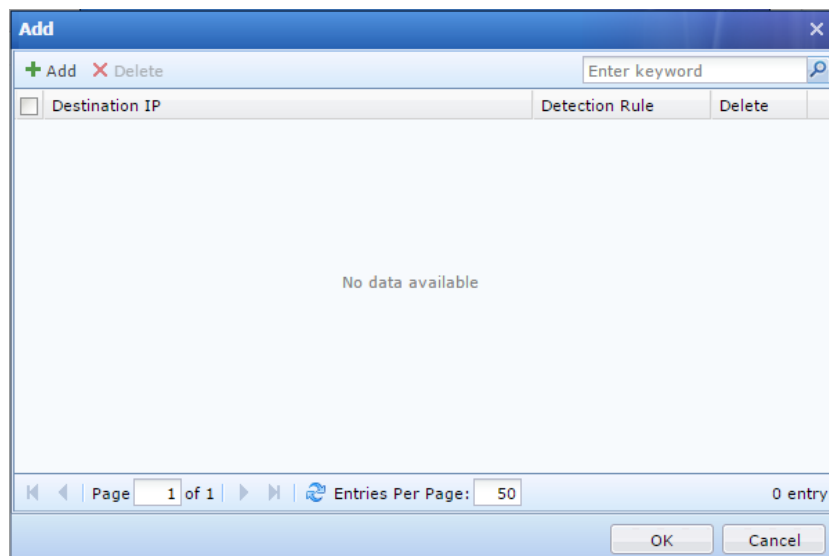
Click on the **Advanced**;  **Advanced** which shown on the **APT detection** page and the page below is prompted:



Globally Excluded Domain/IP: It excludes IP addresses and domain names on the Internet or intranet from anti-malware protection. The device does not block the packets from the specified IP addresses or domains though the packets are zombie network packets. See the following figure:

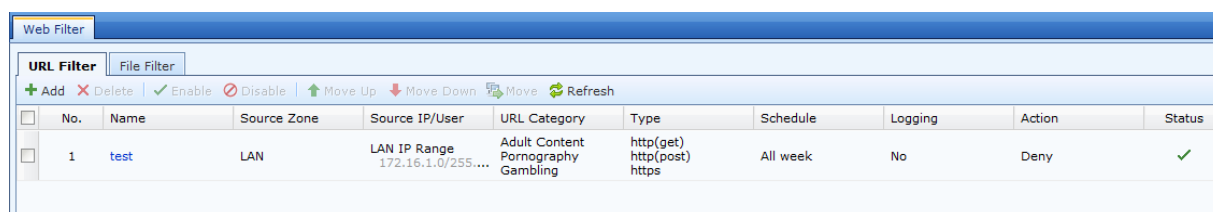


Abnormal Traffic Detection Rule Exclusion: It is only applicable to abnormal connection. Detection based on specified rule will not be applied to connections to the destination IP address.



Web Filter

Web filter is used to filter the access data of web pages that meet criteria. It includes URL filter and file filter. See the following figure:



URL Filter

URL filter is mainly used to filter the URLs of web pages that meet criteria. Access the **URL Filter** page and click Add. See the following figure:

Name: It specifies the name of a rule.

Description: It specifies the description of a rule.

Source Zone and IP/User: You can set the intranet as the source zone and include all users. In this case, the device matches all data from the intranet with specified URLs from top to bottom in the URL list and does not match data from the Internet.

URL Category: It specifies the URL library for URL filter. The built-in and customized objects in **Object Definition > URL Category Library** are invoked.

Type: It specifies the type of URL for the filter, including **HTTP (get)**, **HTTP (post)**, and **HTTPS**. For example, to prevent intranet users from browsing a certain type of web page, select **HTTP (get)**. To allow intranet users to browse web pages but prevent them from uploading files to websites (such as posting on BBS websites), select **HTTP (post)**. To prevent intranet users from browsing HTTP websites, select **HTTPS** and **HTTP (get)**. To allow them to browse the websites but prevent them from uploading files to the websites, select **HTTPS** and **HTTP (post)**.

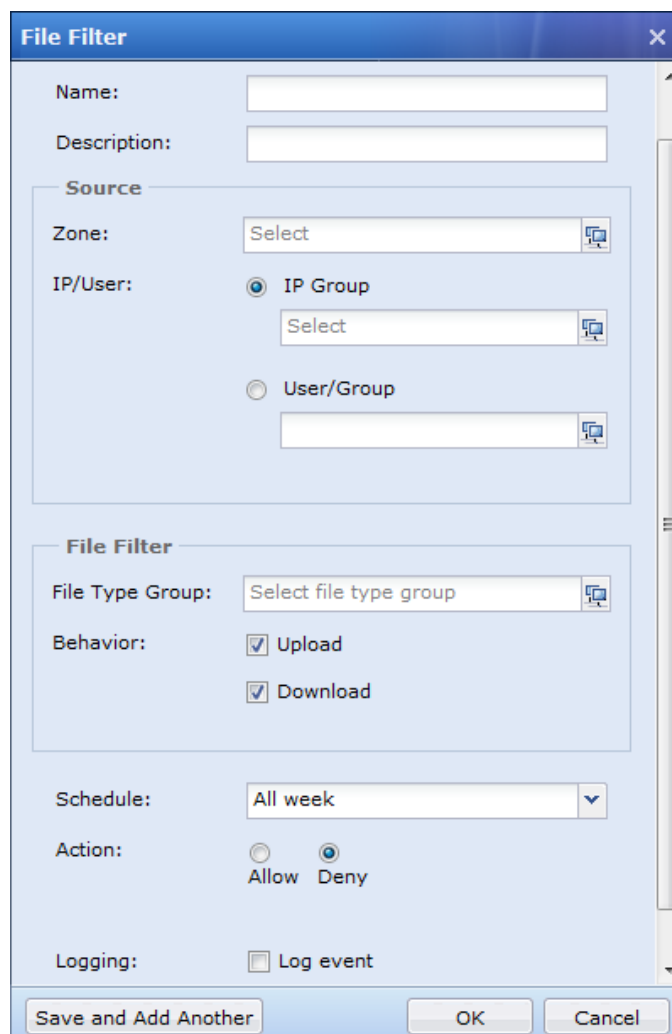
Schedule: It specifies the time when the rule is effective.

Action: It specifies whether the packets meeting the preceding criteria are discarded or not.

Log: URL access actions of users are recorded in the embedded data center when this option button is selected.

File Filter

File filter is used to filter files of specified types downloaded or uploaded through HTTP. For example, it can be used to prevent intranet users from downloading movie files during business hours. See the following figure:



The screenshot shows a 'File Filter' configuration window with the following fields and options:

- Name:** A text input field.
- Description:** A text input field.
- Source:**
 - Zone:** A dropdown menu with 'Select' as the current value.
 - IP/User:** Two radio buttons: 'IP Group' (selected) and 'User/Group'. Below 'IP Group' is a dropdown menu with 'Select'. Below 'User/Group' is a text input field.
- File Filter:**
 - File Type Group:** A dropdown menu with 'Select file type group' as the current value.
 - Behavior:** Two checked checkboxes: 'Upload' and 'Download'.
- Schedule:** A dropdown menu with 'All week' as the current value.
- Action:** Two radio buttons: 'Allow' and 'Deny' (selected).
- Logging:** A checkbox labeled 'Log event'.

At the bottom of the window are three buttons: 'Save and Add Another', 'OK', and 'Cancel'.

Name: It specifies the name of a rule.

Description: It specifies the description of a rule.

Source Zone and IP/User: If the intranet is set as the source zone and all IP addresses are selected, all the data transferred from the intranet through the device is matched with the specified file types from top to bottom in the list. Data from the Internet is not matched.

File Type Group: It specifies the types of files to be filtered.

Behavior: It specifies the behavior of uploading or downloading files through HTTP.

Schedule: It specifies the time when the rule is effective. It can be a repeated period or a specified time.

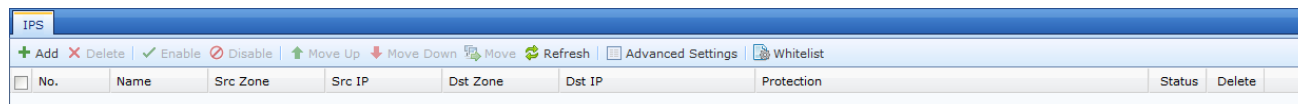
Action: It specifies whether the packets meeting the preceding criteria are discarded or not.

Logging: File filter actions are recorded in the embedded data center when this option button is selected.

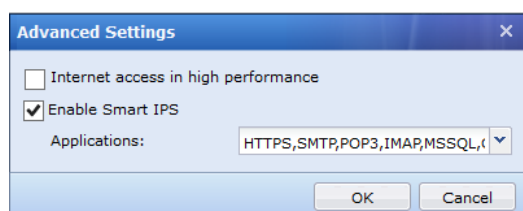
IPS

The Intrusion Prevention System (IPS) checks packets for potential threats on intranet systems. IPS checks the packets entering a network for the real purposes of the packets, and then determines whether the packets can enter the network based on configuration.

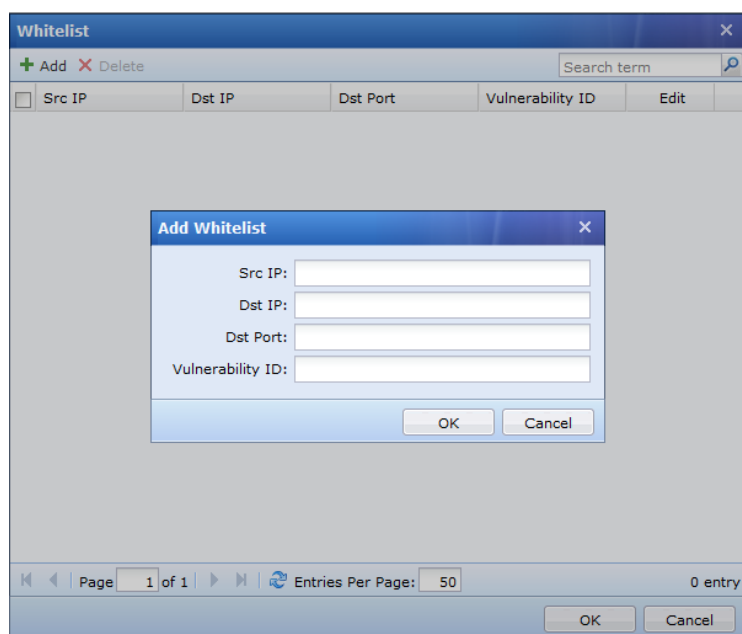
The SANGFOR NGAF device has built-in IPS rules, which can be directly invoked to implement server loophole protection. The following figure shows the configuration page.



Select **Advanced Settings** > **Enable Smart IPS** is selected, loopholes are identified based on applications. Otherwise, loopholes are identified based on port numbers.



Select **Whitelist** to add exception from IPS detection.



Click **Add**. The **Add IPS Rule** page appears. See the following figure:

The 'Add IPS Rule' dialog box is shown. It includes fields for Name, Description, Source (Zone, IP Group), Destination (Zone, IP Group), Protection (Server Protection, Endpoint Protection, Brute-Force attack), Action (Allow, Deny), IP Lockout (Affiliated Source Lockout), and Logging (Log event). The 'Enable' checkbox is checked. The 'Deny' radio button is selected. The 'Log event' checkbox is checked. The 'Save and Add', 'OK', and 'Cancel' buttons are at the bottom.

Enable: The IPS rule is enabled when this option button is selected.

Name: It specifies the name of an IPS rule.

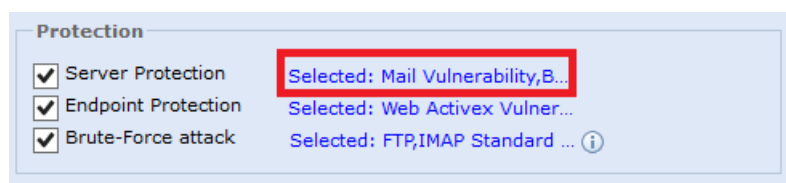
Description: It specifies the description of an IPS rule.

Source Zone and **Source IP Group:** It specifies the source zone and source IP group of data to be matched with the rule for protection. For example, if you set a public zone as the source zone, the loophole attacks from Internet users on servers can be detected.

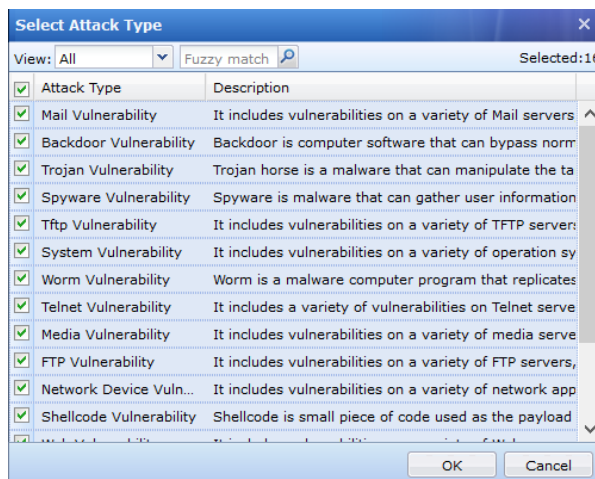
Destination Zone and **Destination IP Group:** Only the IP addresses in the specified IP group in the specified zone are matched with the rule. Usually, the parameters are set to the objects to be protected.

Protection: It specifies the protected content.

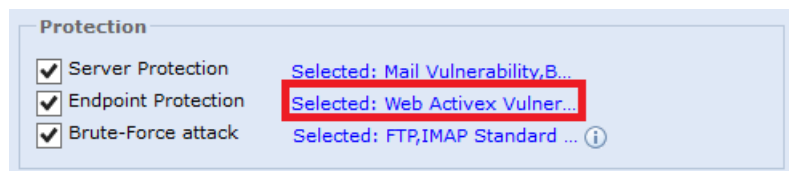
Select **Server** and click **Selected: Mail Vulnerability**.



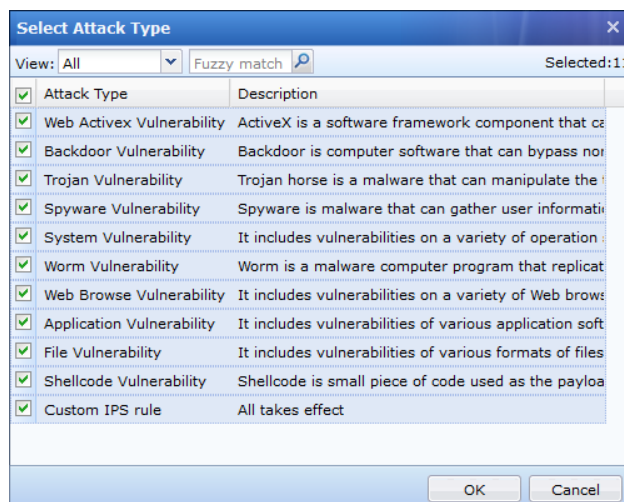
The **Select Attack Type** page appears. Select the attack types based on the services published by the servers so that the device implements IPS protection for the loopholes related to the attack type.



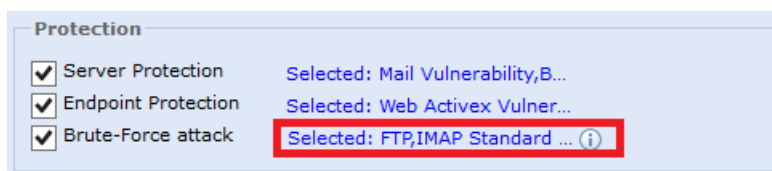
Select **Endpoint** and click **Selected: Web Activex Vulnerability**.



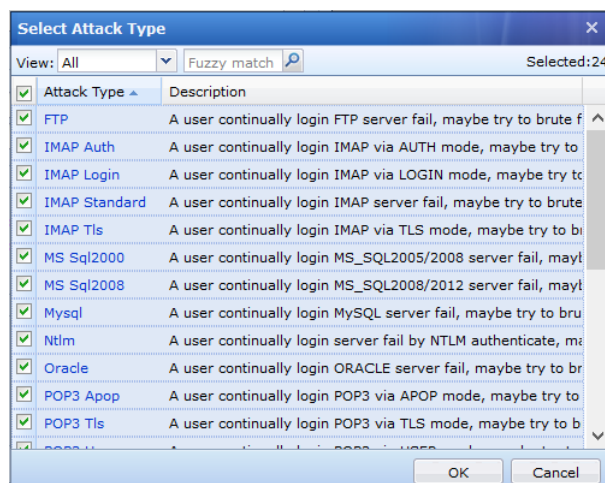
The **Select Attack Type** page appears. Select the attack types so that the device implements IPS protection for the loopholes related to the attack type of endpoints.



Select **Brute-Force Attack** and click **Selected: FTP,IMAP Standard**.



The **Select Attack Type** page appears. Select the attack types so that the device implements IPS protection for the related brute-force attacks.

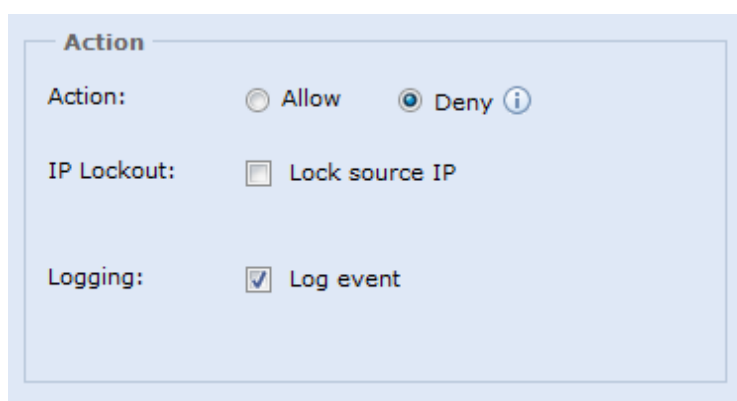


Action area: It specifies whether packets are denied when IPS attacks on protected objects are detected and whether the action is recorded in the embedded data center.

Action: If **Allow** is select, packets are transferred. If **Deny** is selected, packets are discarded.

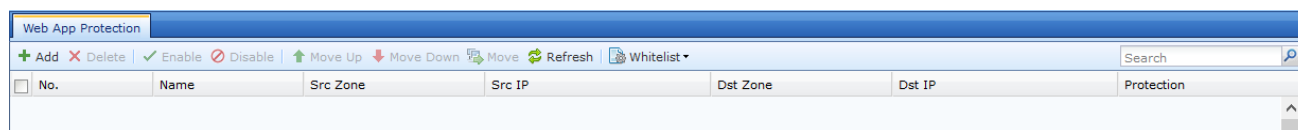
IP Lockout: If Lock source IP is selected, the source IP address initiating attacks is locked when IPS, WAF, or data anti-leak module detects the attacks.

Logging: If **Log event** is selected, attacks by IPS attack packets are recorded in the embedded data center.

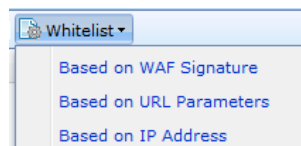


Server Security

Web Application Protection

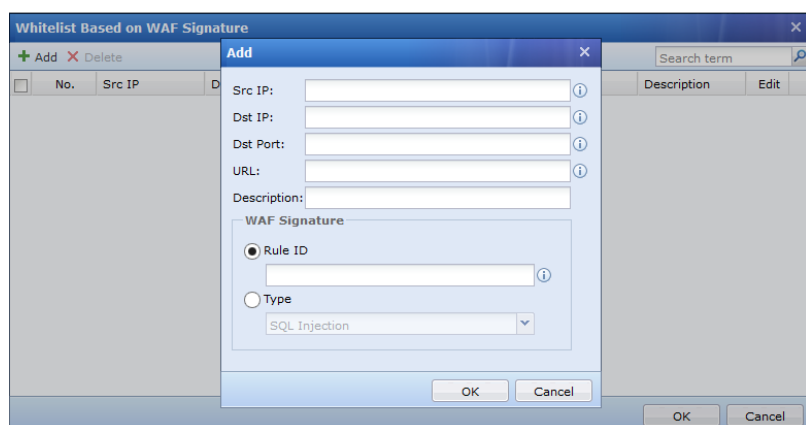


The **Whitelist** is used to exclude from WAF Protection based on 3 types of parameters which are **Signature**, **URL Parameters** and **IP Address**.



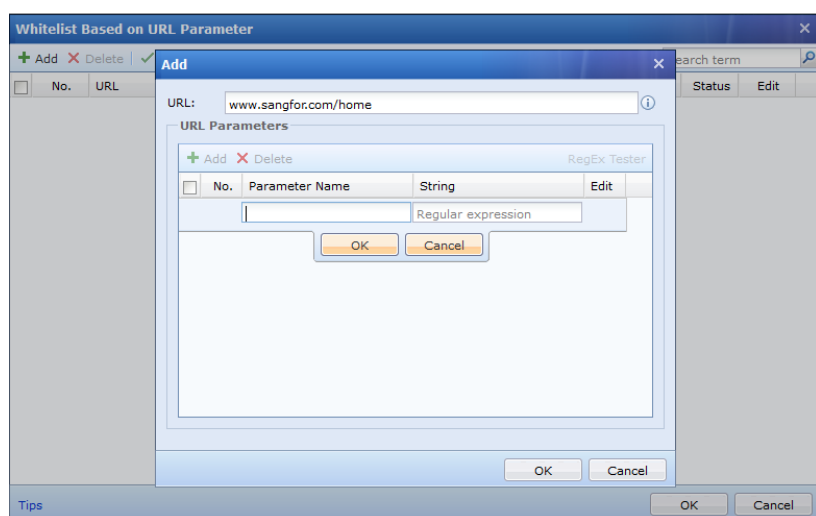
Based on WAF Signature

Fill the required information and WAF Signature Rule ID to whitelist from WAF Protection.



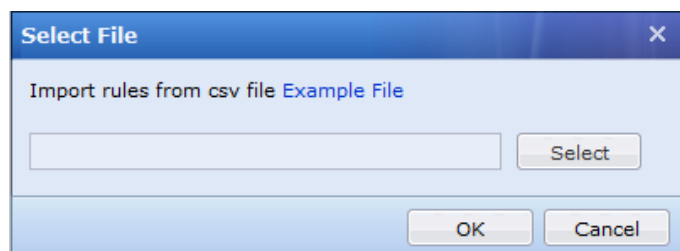
Based on URL Parameters

Fill in the URL with parameter name and string to whitelist from WAF Protection.

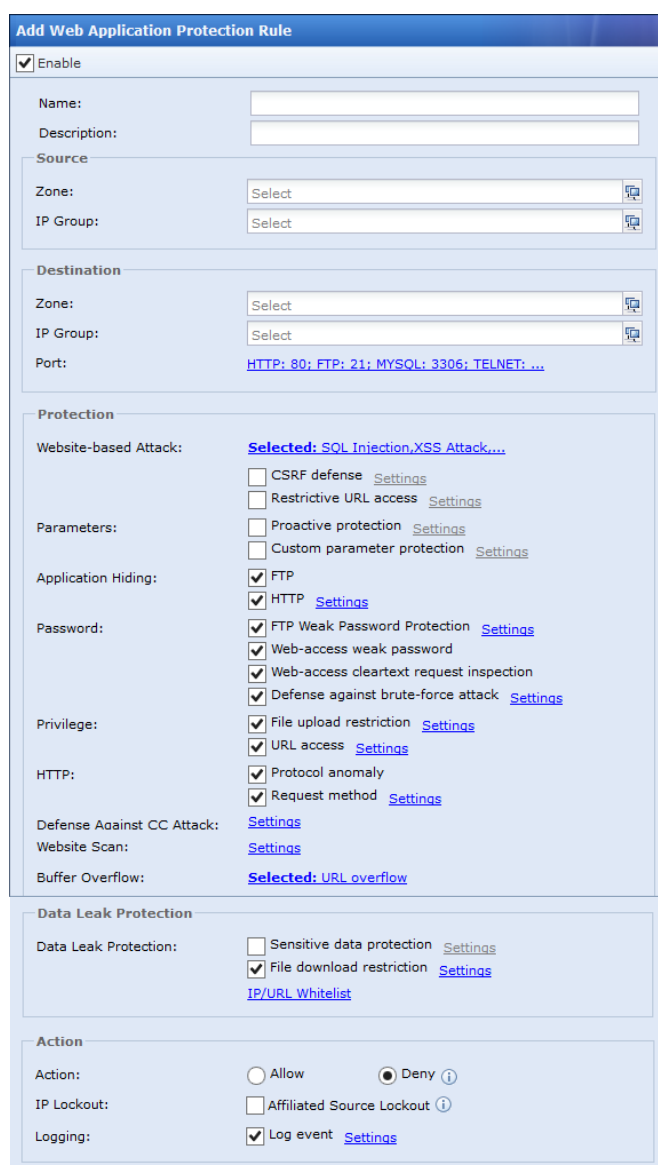


Based on IP Address

Select the csv file to import the IP addresses. The “Example File” can be clicked to download the template.



Web application protection implements attack protection rules designed for web servers on intranets. It can prevent various web application attack behaviors such as OS command injection, SQL injection, and XSS attacks and implement anti-leak configuration for web servers. See the following figure:



Add Web Application Protection Rule

☒ Enable

Name:

Description:

Source

Zone:

IP Group:

Destination

Zone:

IP Group:

Port: [HTTP: 80; FTP: 21; MYSQL: 3306; TELNET: ...](#)

Protection

Website-based Attack: [Selected: SQL Injection,XSS Attack,...](#)

☐ CSRF defense [Settings](#)

☐ Restrictive URL access [Settings](#)

Parameters: ☐ Proactive protection [Settings](#)

☐ Custom parameter protection [Settings](#)

Application Hiding: ☒ FTP

☒ HTTP [Settings](#)

Password: ☒ FTP Weak Password Protection [Settings](#)

☒ Web-access weak password

☒ Web-access cleartext request inspection

☒ Defense against brute-force attack [Settings](#)

Privilege: ☒ File upload restriction [Settings](#)

☒ URL access [Settings](#)

HTTP: ☒ Protocol anomaly

☒ Request method [Settings](#)

Defense Against CC Attack: [Settings](#)

Website Scan: [Settings](#)

Buffer Overflow: [Selected: URL overflow](#)

Data Leak Protection

Data Leak Protection: ☐ Sensitive data protection [Settings](#)

☒ File download restriction [Settings](#)

[IP/URL Whitelist](#)

Action

Action: ☐ Allow ☒ Deny [?](#)

IP Lockout: ☐ Affiliated Source Lockout [?](#)

Logging: ☒ Log event [Settings](#)

Name: It specifies the name of a rule.

Description: It specifies the description of a rule.

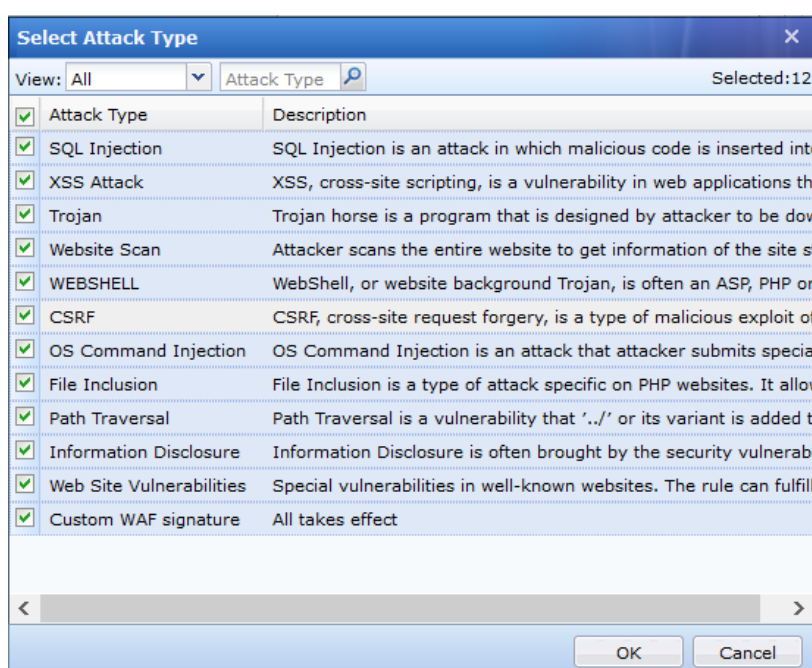
Source Zone: It specifies the source zone of data that is matched with the rule. For example, if you set the Internet as the source zone, it can detect loophole attacks from Internet users on servers.

Destination Zone and Destination IP Group: Only the IP addresses in the specified IP group in the specified zone are matched with the rule. Usually, the parameters are set to the objects to be protected, such as the IP addresses of servers on the intranet.

Port: It specifies the port of the server to be protected. When a user accesses the port of the server, attack detection is implemented.

Website-based attack: It specifies the server attacks to be protected.

Click **Selected: SQL injection, XSS attack**. The **Select Attack Type** page appears. Select the required attack types so that the device can provide related protection.



SQL injection: Attackers take advantage of design flaws to attach SQL code to text boxes on web pages to obtain network resources or change data. The NGAF device can detect such attacks.

XSS attack: Cross-site scripting is a common web application attack on computer security loopholes. It allows injection of code into pages provided for users. For example, it may be contained in HTML code and client scripts to use XSS loopholes to avoid access control and obtain data such as accounts. The NGAF device can detect such attacks.

Trojan horse: Web page Trojan horse is an HTML page fabricated by a hacker. When a user accesses the web page, the script embedded in the web page uses browser loopholes to make the browser download the Trojan horse deployed by the hacker on the Internet and run the Trojan horse. The NGAF device can detect such attacks.

Website scan: It scans websites, as well as the structure and loopholes of the websites. The NGAF device can detect such attacks.

WEBSHELL: It is a script tool for web invasion. Generally, it is an ASP, PHP, or JSP page and is also called website background Trojan horse. After invading a website, a hacker usually deploys the Trojan horse in a web

directory of the server together with web page files, to manipulate the website in a long time. The NGAF device can detect such attacks.

CSRF: It takes advantage of trusted websites by imitating requests from trusted users. The NGAF device can detect such attacks.

OS command injection: An attacker uses the OS loopholes of a server to send OS commands by means of web access to the server to obtain network resources or change data. The NGAF device can detect such attacks.

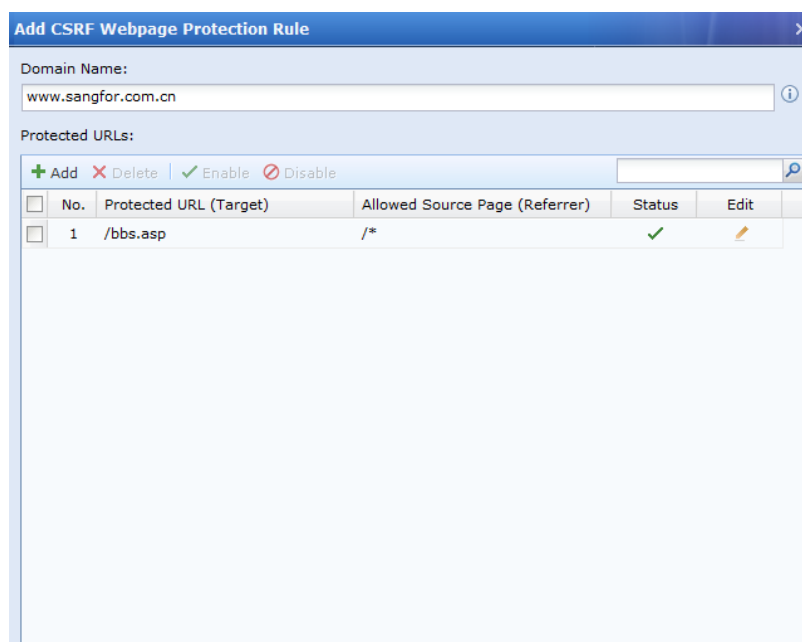
File inclusion: It is a type of attack targeting only PHP websites. If PHP variables are not carefully filtered and local server parameters are not distinguished from remote server parameters, an attacker can use files on remote servers as parameters for variable settings. If the files contain malicious code or PHP Trojan horses, the code or Trojan horses are executed with web permissions. The NGAF device can detect such attacks.

Path traversal: It accesses directories of a web server other than the root directories by using a browser to attach .../ to any directory of the server, attach .../ to a directory with special significance, or attach a variant of .../. The NGAF device can detect such attacks.

Information disclosure: Because of web server configuration or web server security loopholes, some system files or configuration files are directly exposed on the Internet, causing disclosure of sensitive web server information such as user names, passwords, source code, server information, and configuration information. The NGAF device can detect such attacks.

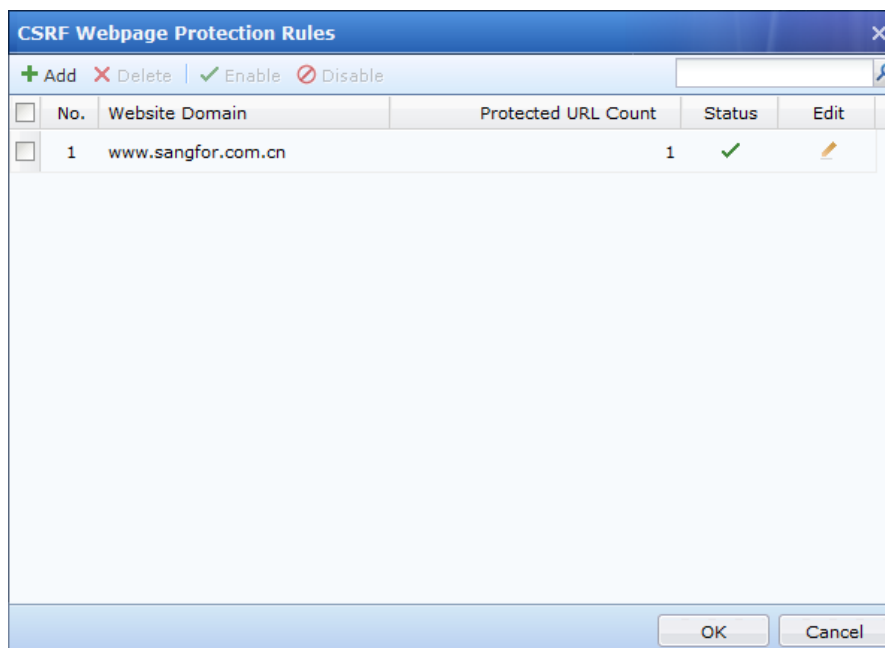
Web site vulnerabilities: Highly reliable protection is implemented for specified loopholes of famous website systems.

Cross Site Request Forgery is also called one click attack or session riding. It is often abbreviated as CSRF or XSRF. It implements attacks by executing malicious operations on web applications to which users have logged in. CSRF protection can effectively prevent such attacks. See the following figure:



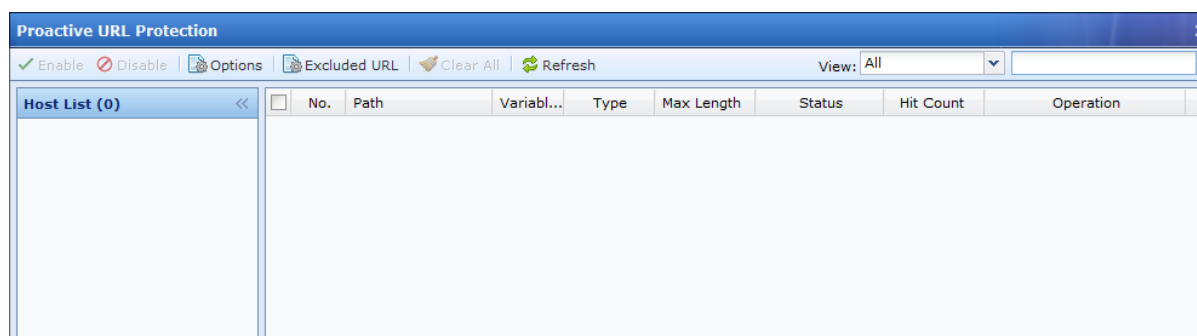
Specify the domain names to be protected, added pages to be protected, and source pages that can be accessed to ensure that only redirection from the source pages (Referer) to protected URLs (Target) can be implemented. In this way, CSRF attacks are blocked.

Protected URL ensures that users' key resources cannot be browsed by unauthorized clients. See the following figure:



Only www.sangfor.com.cn/bbs/index.html can be redirected to www.sangfor.com.cn, which cannot be accessed by other means.

Parameter Protection-Proactive URL Protection: Tradition SQL injection is implemented based on characteristics. SQL injection protection systems based on characteristics cannot resolve the Oday and unknown attack problems. Therefore, proactive URL protection is added to the device to improve AF security protection. See the following figure:



You only need to enable the protection. The device can learn protection itself. When **Variable Hits Threshold** is reached, it binds related parameters.

Options

Learning Ability ⓘ

Variable Hits Threshold: times

Matching Ratio ⓘ

Ratio: %

Action if Attack Attempt Detected

☐ Deny ☒ Log event

OK Cancel

Results:

Proactive URL Protection

✓ Enable ✗ Disable Options Excluded URL Clear All Refresh View: All

No.	Path	Variabl...	Type	Max Length	Status	Hit Count	Operation
1	/cms/plus/list.php	tid	Being lea...	2	Being learned	3	Edit Learn Again URL Whi...
2	/cms/plus/view.p...	aid	Being lea...	2	Being learned	1	Edit Learn Again URL Whi...

Host List (1) << >> sangforserver.no-ip.org (2)

Page 1 of 1 Entries Per Page: 50 1-2 of 2 Close

Parameter Protection-Custom Parameter Protection Rule: Similar to proactive URL protection, only the related parameters must be set. Regular expressions are supported. When the conditions specified by regular expressions are met, actions are denied.

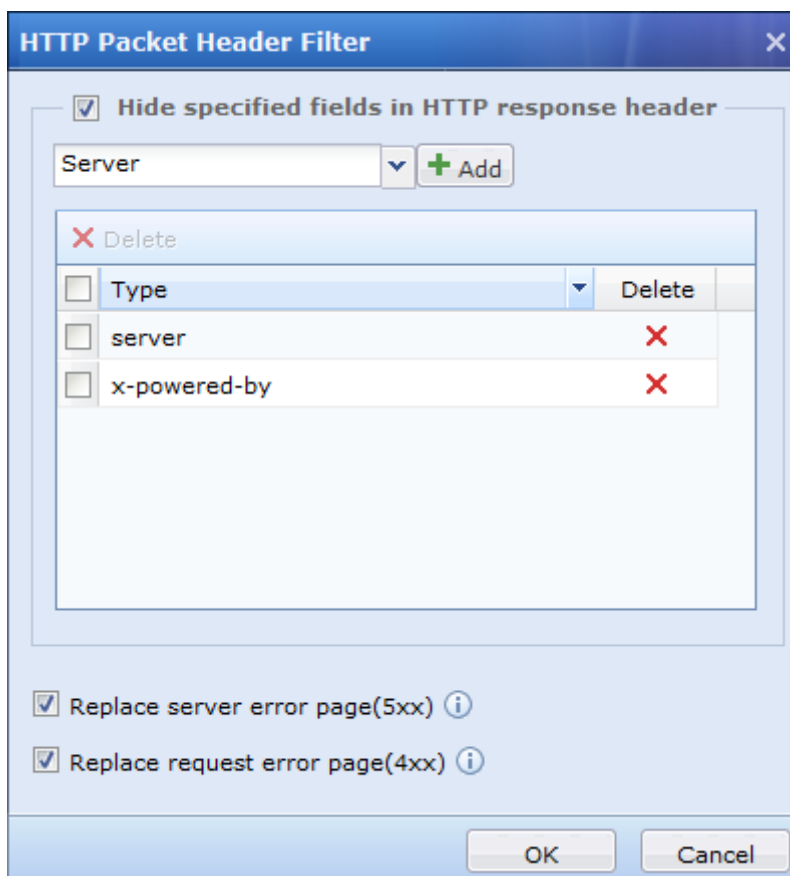
Custom Parameter Protection Rule

+ Add ✗ Delete ✓ Enable ✗ Disable

No.	URL	Case Sen...	Variables, Definition, Value	Status	Edit
1	/admin.asp	Yes	id, is ,URL	✓	

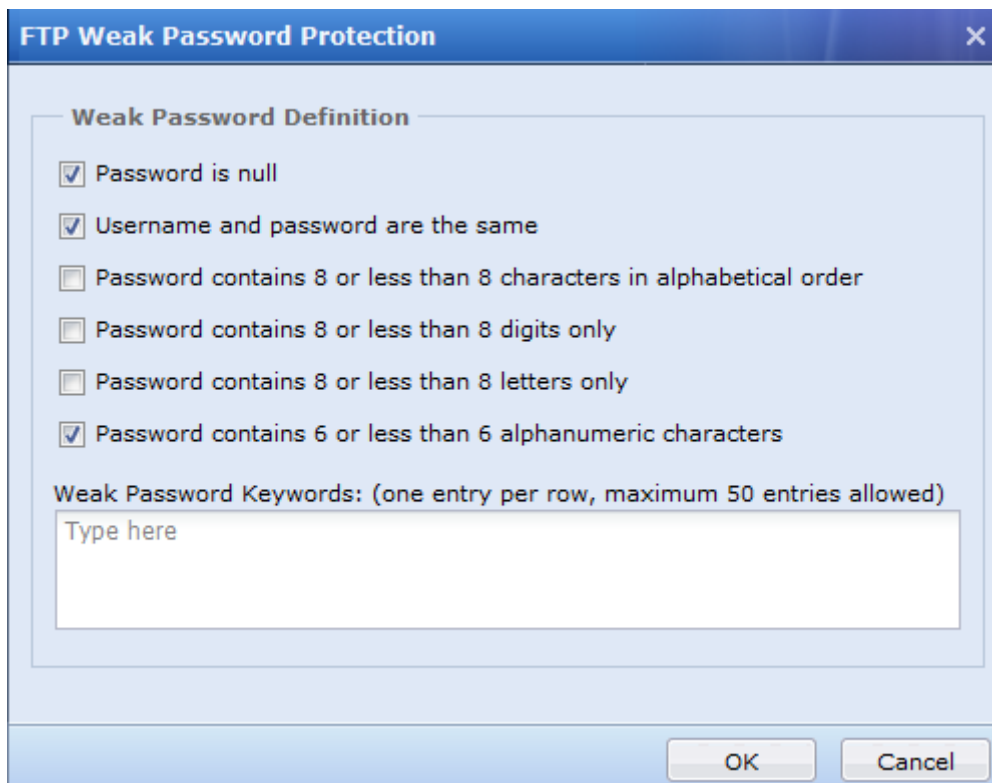
Application Hiding-FTP: When a client logs in to the FTP server, the server sends back information such as version to the client. An attacker can use the loopholes related to the version to initiate attacks. This function hides the information sent back to prevent attacks. To hide the information, select **FTP**.

Application Hiding-HTTP: When a client accesses a website, the server sends many fields contained in HTTP headers to the client, such as **Server** and **Via**. **Via** may cause disclosure of proxy version information. An attacker can use the loopholes of the related version to initiate attacks. Therefore, the fields can be hidden to prevent attacks. Select **HTTP**, and click **Settings**. The page shown in the following figure appears.



Customize the content of the HTTP header. You can use packet capturing tools such as HTTPWATCH to obtain some fields sent back by the server to the client and enter the fields on this page. Select **Replace server error page** to enable the firewall to replace an error information page (such as error 500 page) that usually contains server information sent from the server with an error information page that does not contain server information.

FTP Weak Password Protection: It is applicable only to the FTP protocol. It filters simple user names and passwords. Select **FTP Weak Password Protection** and click **Settings**. The page shown in the following figure appears.



Select the required rules or enter a weak password list, and then click **OK**. When the firewall detects a weak password, the client cannot log in to the FTP server with the password. The password must be changed on the FTP server to another one that meets requirements or the firewall password rule must be changed to resolve the problem.

Web Weak Login Password Protection: It implements weak password protection during web login. Enable this function.

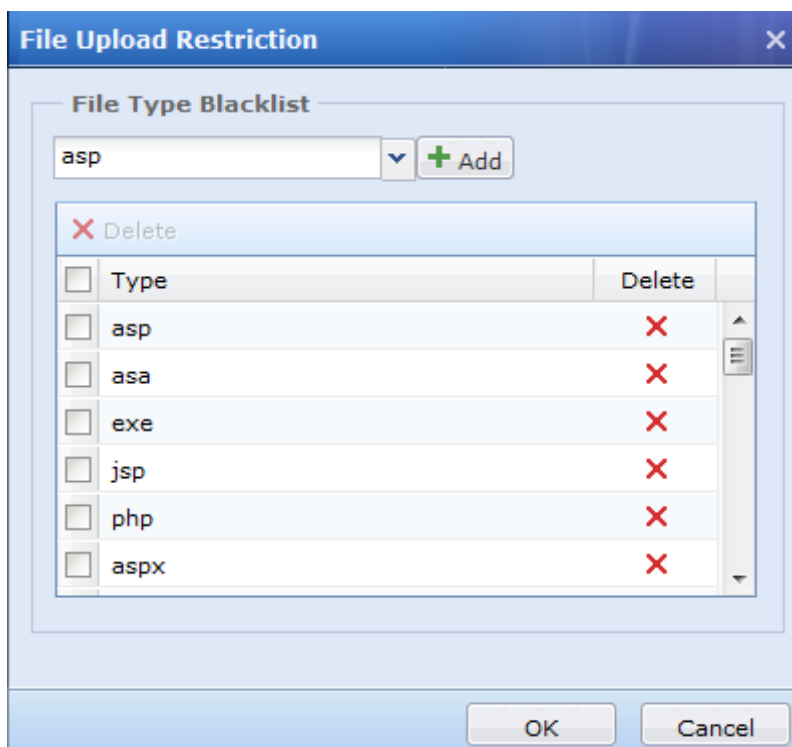
Web Login Plain Text Transfer Detection: It implements plain text transfer detection during web login. Enable this function.

Defense against Brute-Force Attack: It is applicable to the FTP and HTTP protocols. It is used to prevent password cracking. Select **Defense against Brute-Force Attack**, and click **Settings**. The page shown in the following figure appears.



To prevent FTP password cracking, select **FTP**. To prevent HTTP website login password cracking, enter the URLs of the related websites. For example, if the login URL of a website is `http://www.***.com/login.html`, enter `/login.html`. See the preceding figure. **Attempt Count**: It specifies the maximum number of incorrect passwords entered in a minute. If the upper limit is exceeded, the actions are regarded as password cracking attempts.

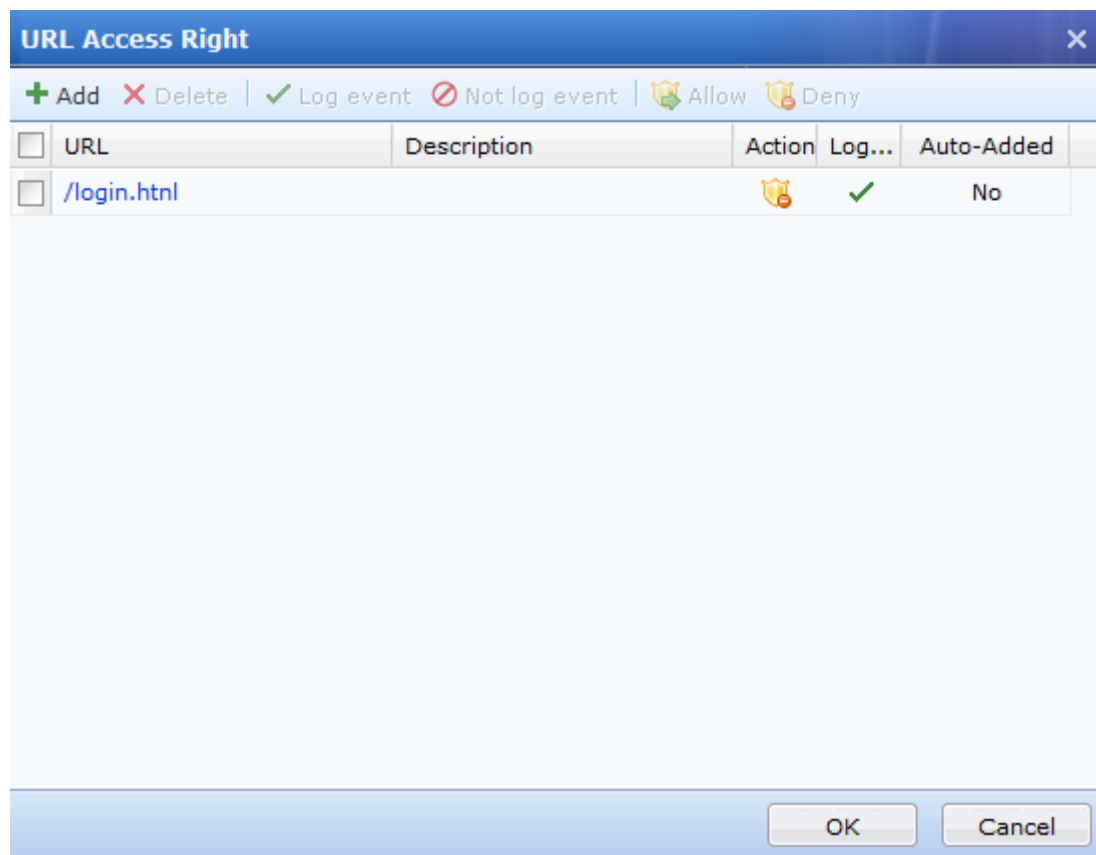
File Upload Restriction: It filters the types of files uploaded by clients to servers. Select **File Upload Restriction** and click **Settings**. The page shown in the following figure appears.



Click  and choose preset file types and click  to add the types to the list. To customize a type, enter it

in the text box and click  to add it to the list.

URL Protection: It is used to set URL access rights. For example, if access to a URL is prohibited, the preceding attack protection measures are ineffective to the URL. The URL will not be attacked because clients cannot access it. If a URL is allowed to be accessed, the preceding attack protection measures are ineffective to the URL. Select **URL Protection**, and click **Settings**. The page shown in the following figure appears.

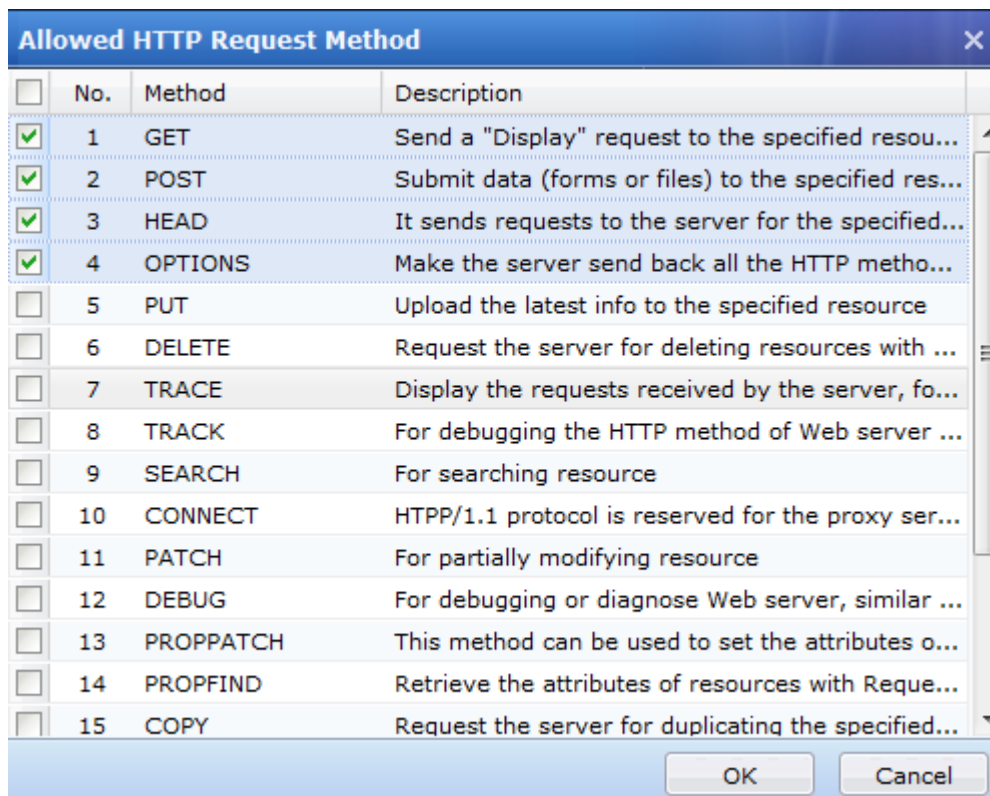


Similar to password cracking protection, you need to enter only the suffixes of URLs. For example, if a URL is `http://www.***.com/login.html`, enter `/login.html`.

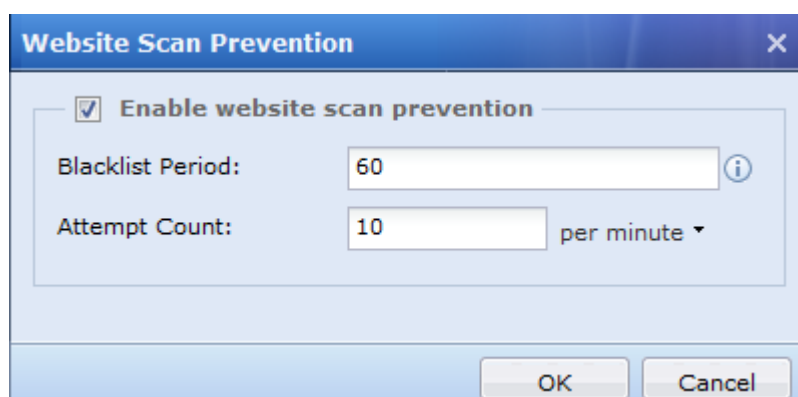
HTTP Exception Detection-Protocol Exception: It prevents the attack caused by incorrect processing by the server of multiple request parameters on ASP or ASPX pages.

HTTP Exception Detection-Method Filter: It specifies allowed HTTP methods. Click **Settings**. The page shown in the following figure appears.

Select the allowed HTTP methods. The HTTP methods not selected are regarded as HTTP exceptions.



Website Scan Prevention: It prevents website scans. See the following figure:



Buffer Overflow Detection: It specifies whether to detect URL overflow, POST entity overflow, and HTTP header overflow. Click [Selected: URL overflow, POST entity overflow.](#) . The **Buffer Overflow Detection** page appears. Select the required detection options. The device then provides protection against the selected types of overflow.

Buffer Overflow Detection

☒ **Check for URL overflow**

Max URL Length (Bytes):

☒ **Check for POST entity overflow**

Max URL Length (Bytes):

☒ **Check for HTTP header overflow**

+ Add - Delete

Field	Max URL Length(B...
No data available	

Select **Check for URL overflow** and set **Max URL Length**. The device then checks URL lengths to prevent buffer overflow.

Select **Check for POST entity overflow** and set **Max URL Length** to prevent overflow resulting from data receiving by servers.

Select **Check for HTTP header overflow**, click **Add**, and set the maximum length of specified fields in HTTP headers. Then, the device checks for the fields with excessive lengths.

Server data leakage (such as the CSDN and Tianya events) is becoming increasingly serious. After deploying the SANGFOR NGAF device, you can enable the data leakage protection function to prevent leakage of sensitive information.

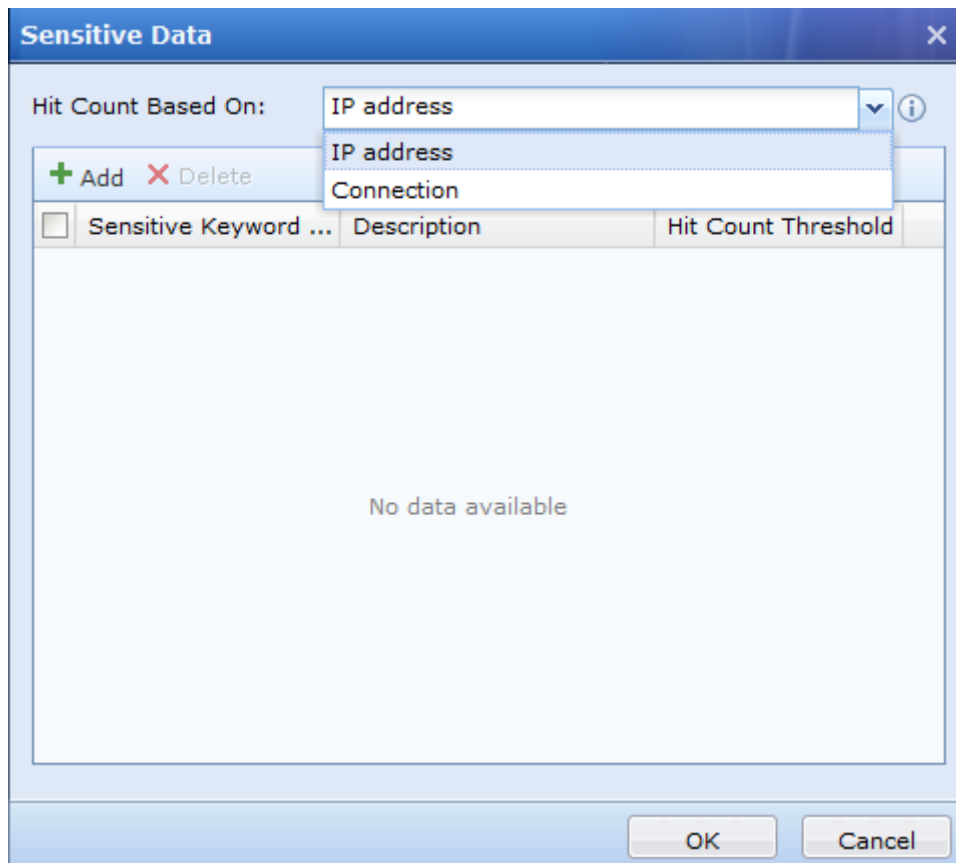
Data Leak Protection

Data Leak Protection: ☒ Sensitive data protection [Settings](#)

☒ File download restriction [Settings](#)

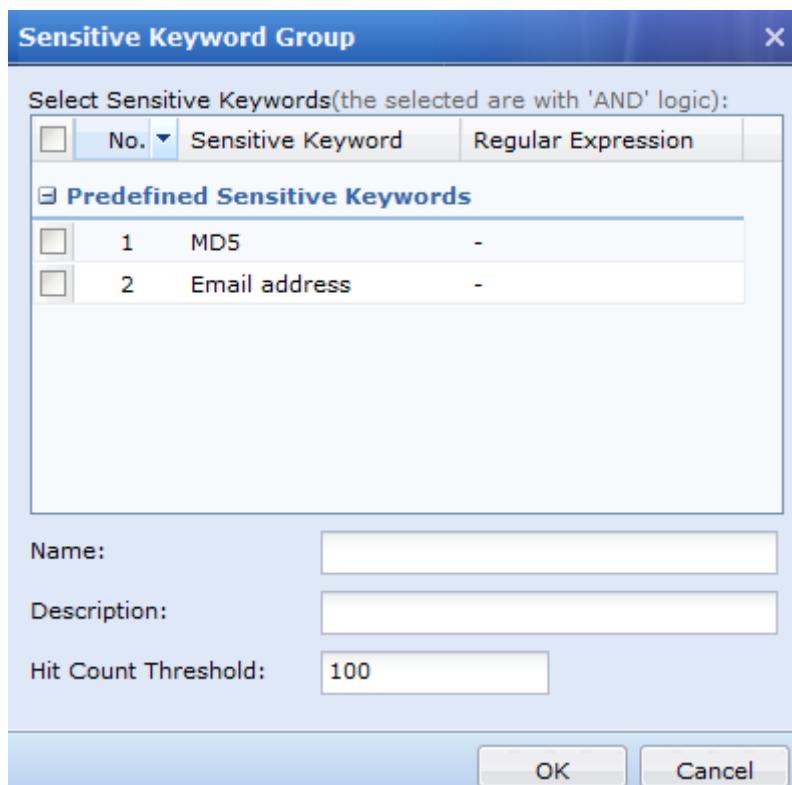
[IP/URL Whitelist](#)

Set **Data Leak Protection** to **Sensitive data protection** and click **Settings**. The **Sensitive Data** page appears. Specify sensitive data and the method of calculating sensitive data hits. See the following figure:



You can set **Hit Count Based On** to **IP address** or **Connection**. **IP address** indicates that when sensitive data is transferred through the device, the hits of an IP address are counted. **Connection** indicates that when sensitive data is transferred through the device, the hits of a connection are counted. When it is set to **Connection**, joint source IP address locking is enabled by default.

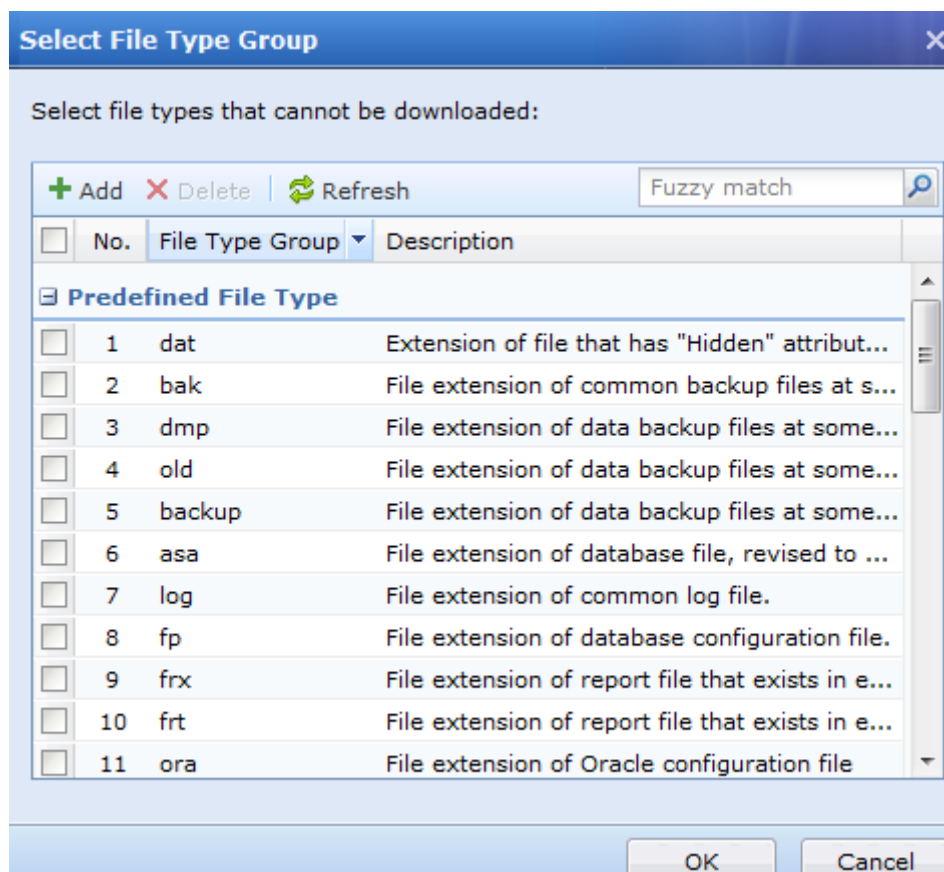
Click Add, select sensitive data, and set sensitive data combination policies. See the following figure:



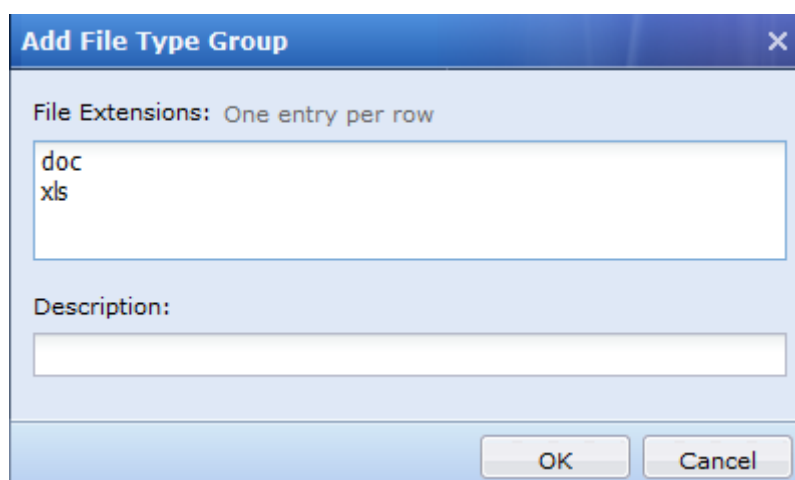
You can add multiple sensitive data combination policies, with each policy called a mode. Each mode can contain multiple pieces of sensitive data. If a mode contains multiple pieces of sensitive data, a hit is counted only when all the sensitive data is matched. When the minimum number of hits is reached or exceeded, it is regarded as sensitive data leak. The modes have the OR relationship. A hit is counted when a mode is matched.

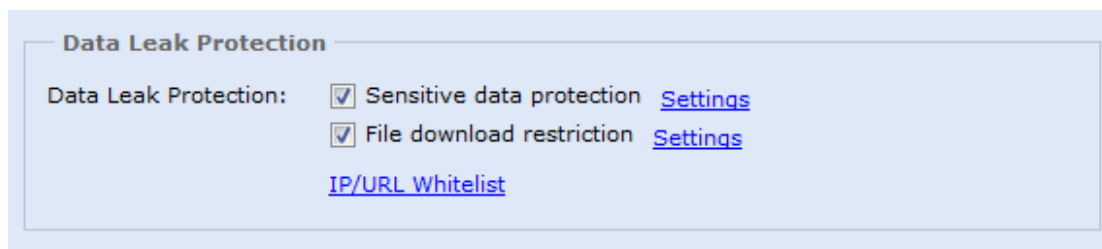
Some sensitive data is stored in Word or Excel files, which may be downloaded from the server and disclosed. The NGAF can prevent such sensitive data leakage by filtering files downloaded.

Set **Data Leak Protection** to **File download restriction** and click **Settings**. The **Select File type Group** page appears. Select the extensions of files to be filtered. See the following figure:



The device is preset with extensions of some common website data backup files and common log files. To customize an extension, click **Add** and add the extension. See the following figure:

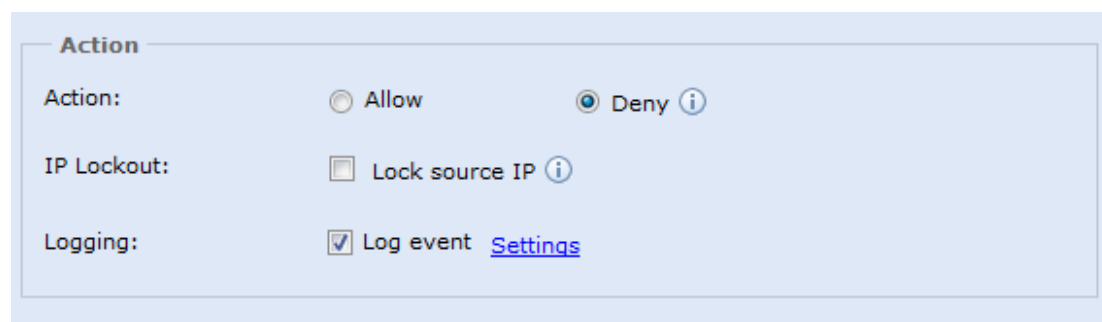




Data Leak Protection

Data Leak Protection: ☒ Sensitive data protection [Settings](#)
☒ File download restriction [Settings](#)
[IP/URL Whitelist](#)

Click [IP/URL Whitelist](#) on the data leak protection configuration page, and configure exclusion settings for specified IP addresses or URLs. For details about object protection exclusion, see section 3.4.3.1.



Action

Action: ☐ Allow ☒ Deny [i](#)

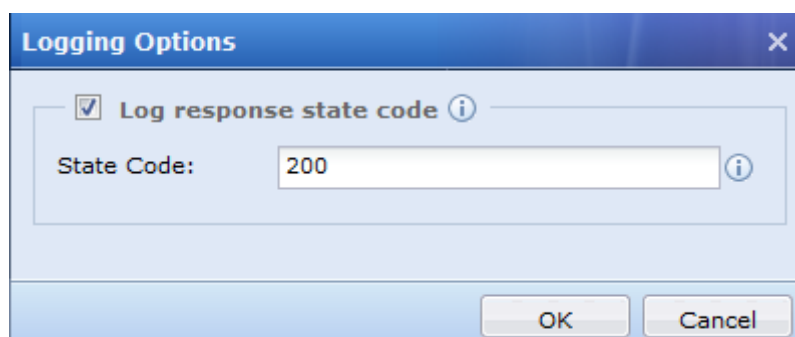
IP Lockout: ☐ Lock source IP [i](#)

Logging: ☒ Log event [Settings](#)

Action: If **Allow** is selected, attacks are detected only. If **Deny** is selected, attacks are both detected and blocked.

IP Lockout: If **Lock source IP** is selected, the source IP address initiating attacks is locked when IPS, WAF, or data anti-leak module detects the attacks.

Logging: If **Log event** is selected, detected attacks are recorded in the data center. You can click **Settings** and set related state code.



Logging Options [X]

☒ Log response state code [i](#)

State Code: [i](#)

OK Cancel



- Only when Deny is selected will the device blocks attacks detected.
- In URL protection, the action Allow and Deny are not related to the action Deny to be taken when attacks are detected. The action set in URL protection prevails.

Server Access Verification

The **Server Access Verification** is used to protect server access. It will require confirmation by email if the user is not in the IP Addresses List.

Example: Only Admin IP (192.200.19.25) does not require authentication confirmation by email, other IPs than this are required email authenticate confirmation.

Server Access Verification					
+ Add - Delete ✓ Enable ✗ Disable ↻ Refresh 📧 Webmaster Email Address					
<input type="checkbox"/>	No.	Name	URL	FTP Auth URL	Status
<input type="checkbox"/>	1	ProtectServer	http://192.200.19.96/login/admin	-	✓

Click **Webmaster Email Address > Add** to add the Webmaster Email Address. See the figure below.

The screenshot displays the 'Webmaster Email Address' window. At the top, there are buttons for '+ Add', '- Delete', and '↻ Refresh', along with a search dropdown set to 'Username'. Below this is a table with columns for 'Username', 'Email Address', and 'Delete'. Two entries are listed: 'Admin' with email 'admin@sangfor.com' and 'wuyuan' with email 'vincent@sangfor.com', both with a status of 'In use'. Overlaid on this is a smaller 'Add Webmaster Email Account' dialog box. This dialog has two input fields: 'Username:' and 'Email Address:'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Username: Name of the person which this email address belongs to.

Email Address: An email address for Authenticate Confirmation to be sent.

Click **Add** to add new Server Access Verification.

Authenticate Confirmation will be sent to the selected **Email Address** in the Webmaster Email Account.

Name: The name of Server Access Verification

Server IP: The IP of Server

Website Protection

CMS Admin Console Access: Tick to enable central management system, so people can access CMS via browser

HTTP Port: The port number of CMS

URL: The URL of CMS

FTP Server Access

FTP Port: The port number of FTP server

URL: The URL of FTP Server

Authentication

Based on IP Address: IP Addresses selected in here do not required any authenticate confirmation by email

Based on Email: Tick to enable authentication based on Email

Email Address: The authenticate confirmation will be sent to the selected Email Address

Valid For: The validity of email can be configure in minutes

Scanners

Risk Assessment

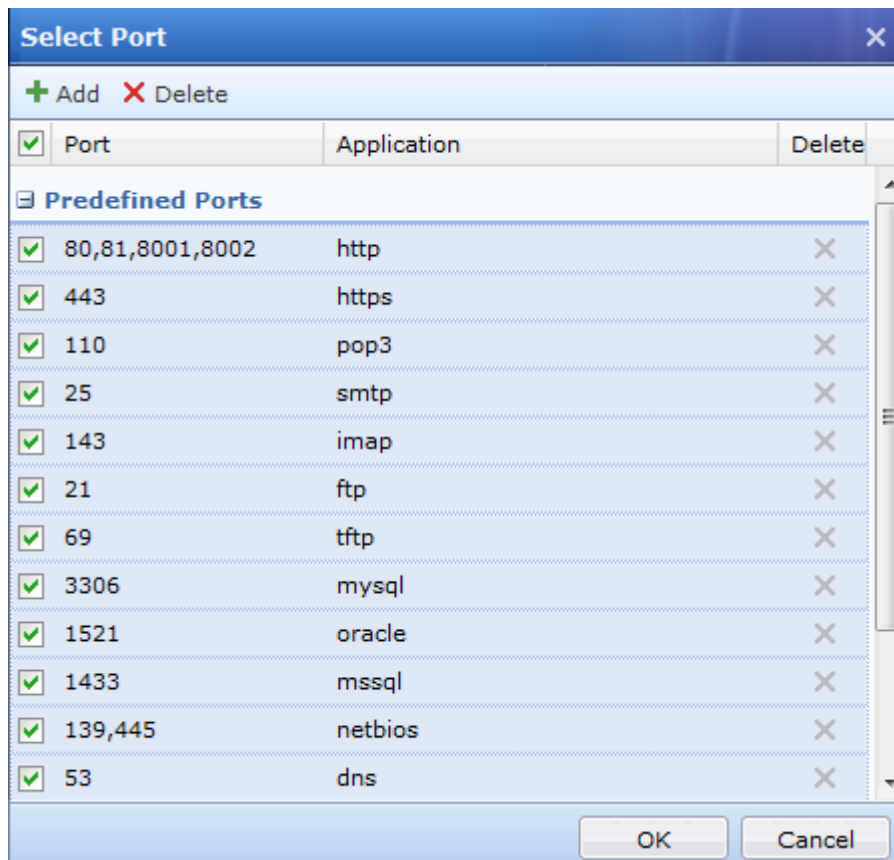
Risk detection and prevention scans ports for destination IP addresses so that administrators know the enabled ports and services of servers as well as all possible server loopholes. Therefore, the administrators can disable unnecessary ports to prevent loopholes, which increases server security. Risk detection and prevention scans for weak passwords for destination IP addresses so that administrator can resolve weak database password problems. Meanwhile, **Risk Assessment** can generate rules based on scan results to provide protection for customers. See the following figure:

The screenshot shows the 'Risk Assessment' interface. It has a blue header bar with the title 'Risk Assessment'. Below the header, there are three input fields: 'Untrusted Source Zone:', 'Destination:', and 'Port:'. The 'Destination:' field contains the text 'IP address or range'. The 'Port:' field contains the text '80,81,8001,8002/http, 443...'. To the right of these fields is a green 'Start' button with a magnifying glass icon. Below the input fields, there is a checkbox labeled 'Enable weak password scan'. At the bottom of the interface, there is a table with the following columns: 'Server IP', 'Port', 'Applic...', 'Protocol', 'Accessibl...', 'Accessible IP', 'Threat Le...', and 'Risk'. The table is currently empty.

Untrusted Source Zone: It defines the source zone for application control policies, IPS, and WAF detection. It is used to check whether application control policies, IPS, and web application protection rules are implemented between the zone and destination IP address.

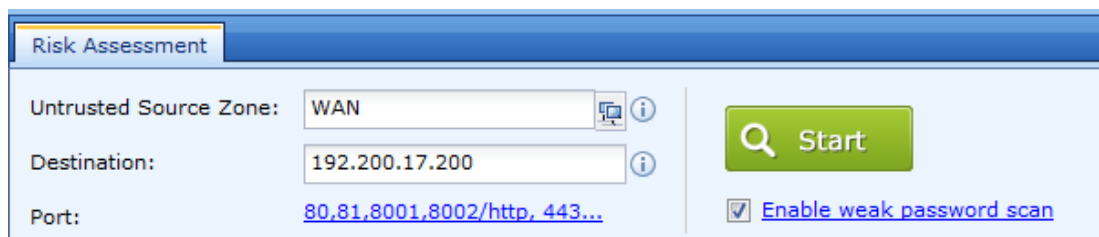
Destination: It defines the range of destination IP address for which ports or weak passwords are scanned.

Port: It defines the ports of destination IP addresses to be scanned. Click **80,81,8001,8002....**. The **Select Port** page appears. See the following figure:

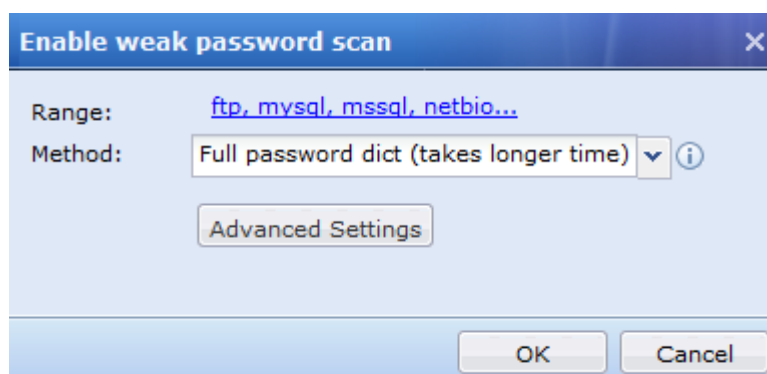


Common ports of servers are preset in the device. To add a port, click **Add**.

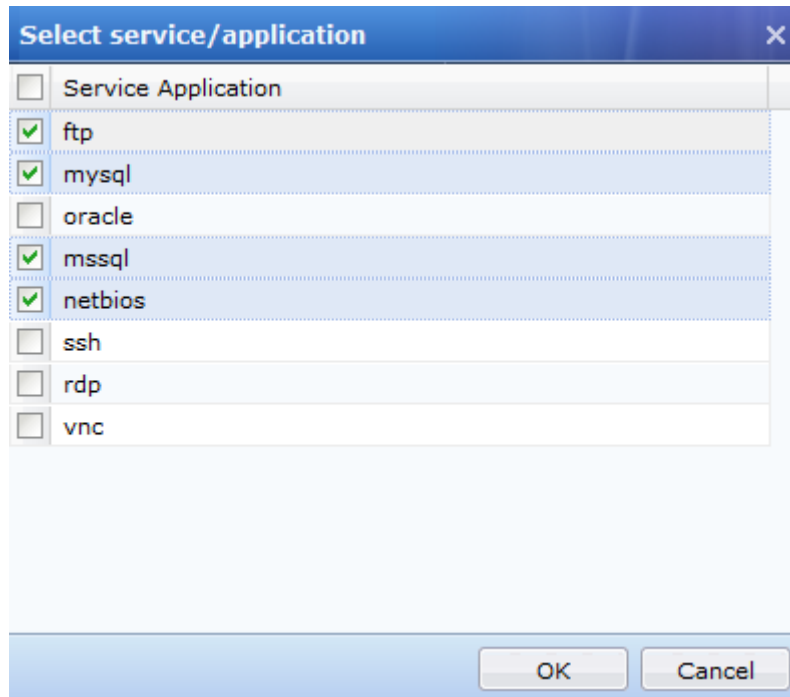
Select **Enable weak password scan** to enable the weak password scan function. See the following figure:



Click **Enable weak password scan**. The **Enable weak password scan** page appears. See the following figure:

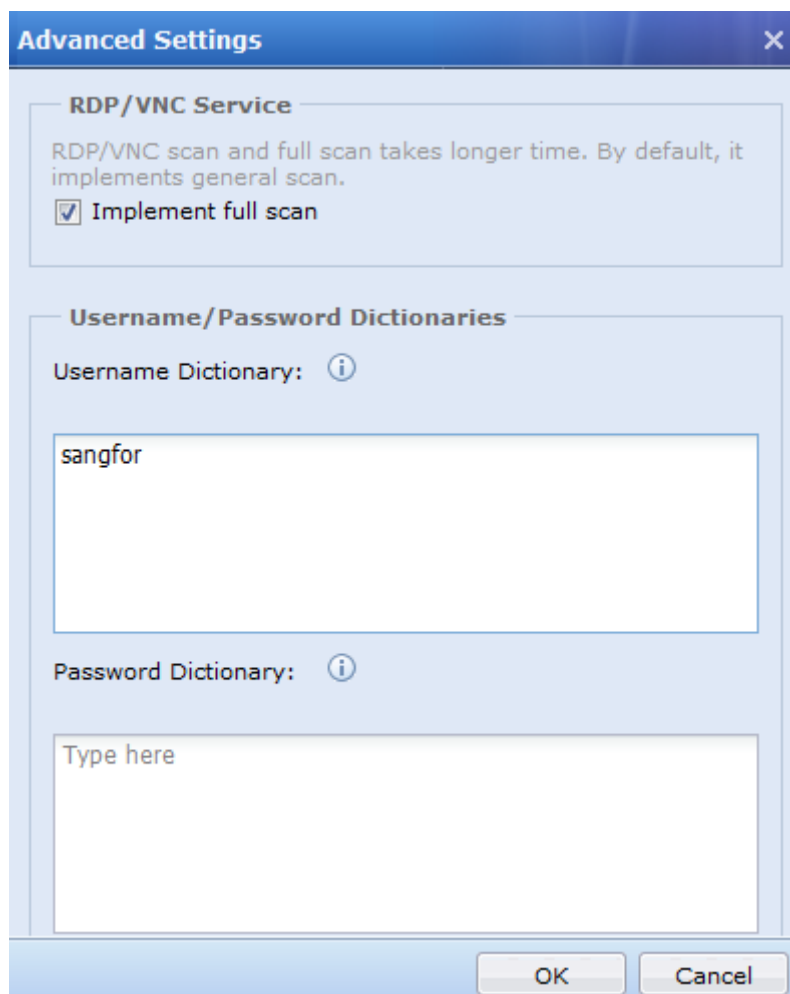


Range: Select the applications and services for which weak passwords are to be scanned.



Method: It defines the method of scanning weak passwords. The values include **Full password dict** and **Normal password dict**. The normal password dictionary contains only default system passwords.

Click **Advanced Settings** and set full password scan and the customized dictionary of RDP and VNC. See the following figure:



Implement full scan: It takes a long time to scan weak passwords for RDP and VNC. To implement full scan for the two protocols, select this option.


Username Dictionary: It defines user names to be found. Add customized user names to the related dictionary. For example, if the user name is **sangfor**, the NGAF device checks whether the user name **sangfor** exists in addition to scanning for weak passwords of default user names.

Password Dictionary: It defines weak passwords to be found. Add customized passwords to the related dictionary. For example, if the password is **sangfor**, the NGAF device checks whether the default user names use the password **sangfor** when scanning for default weak passwords of the default user names.



After port and weak password scan is set, click . The scan result is displayed on the lower part of the page. See the following figure:

<div>Avoid Risk Export as PDF All Associated Policies</div>									
<input type="checkbox"/>	Server IP	Port	Applic...	Protocol	Accessibl...	Accessible IP	Threat Le...	Risk	Operation
<input type="checkbox"/>	192.200.17.200	1433	mssql	TCP	WAN	0.0.0.0-255.255.255.255	High	Open port risk	
<input type="checkbox"/>	192.200.17.200	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	

Click  corresponding to a scan result, the **Port Block Policy** page appears.

Port Block Policy

Source

Source Zone: WAN

Source IP: 0.0.0.0-255.255.255.255

Service

Target Server: 192.200.17.200

Service: TCP/80

Action: Deny

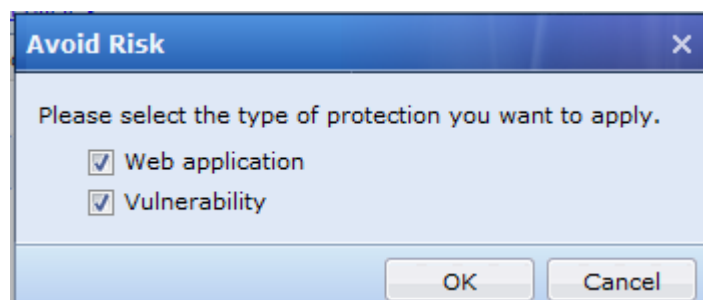
Logging: Log event

OK

Cancel

Click **OK**. The port is blocked and an application control policy for denying access is generated.

Select a scan result and click **Avoid Risk**. The **Avoid Risk** page appears. See the following figure:



Select the risks to be avoided and click **OK**. IPS rules and web application protection rules are generated based on risk instructions.

Click **Export as PDF** to generate a PDF file containing a proactive scan analysis report.

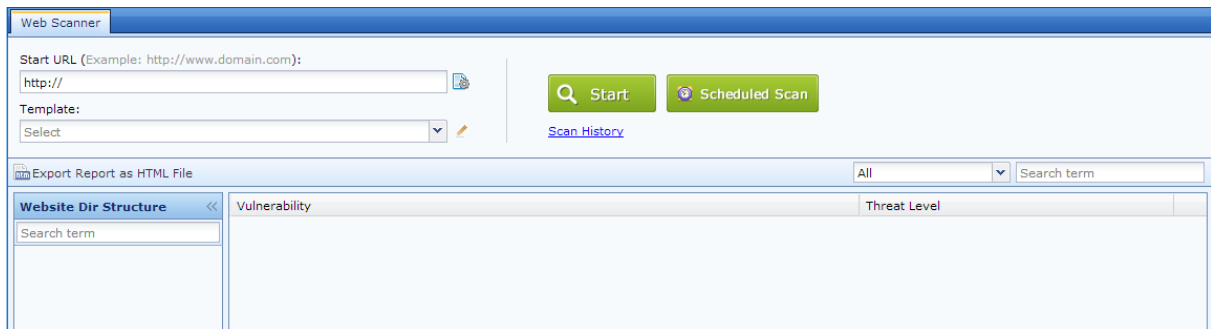
Click **All Associated Policies**. The protection rules generated when **Avoid Risk** is implemented.




You can click a policy name to view the protection rule configuration.

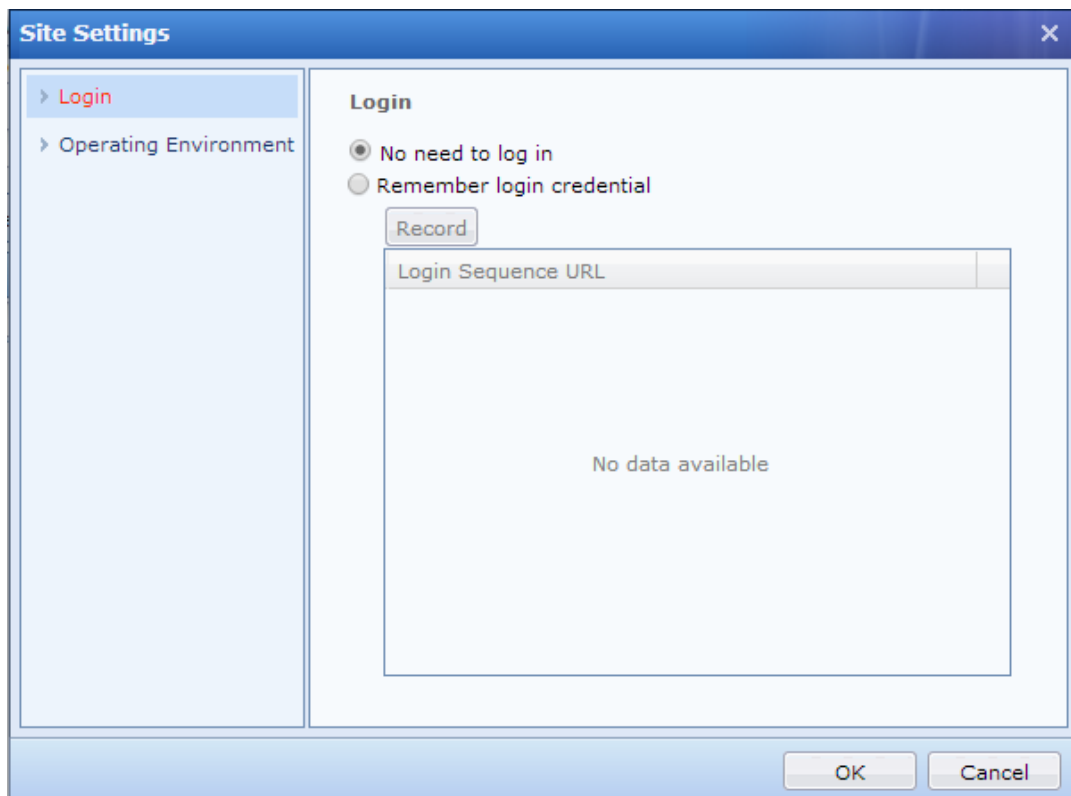
Web Scanner

Web Scanner scans websites and web servers so that administrators know the possible flaws and vulnerabilities that might be exploited by third party and affect the operation of the server. On top of that, the scan results can be exported as a report in HTML file. Therefore, the administrators can take action based on the report to prevent unwanted access and modification on the website, which increases server security. See the following figure:



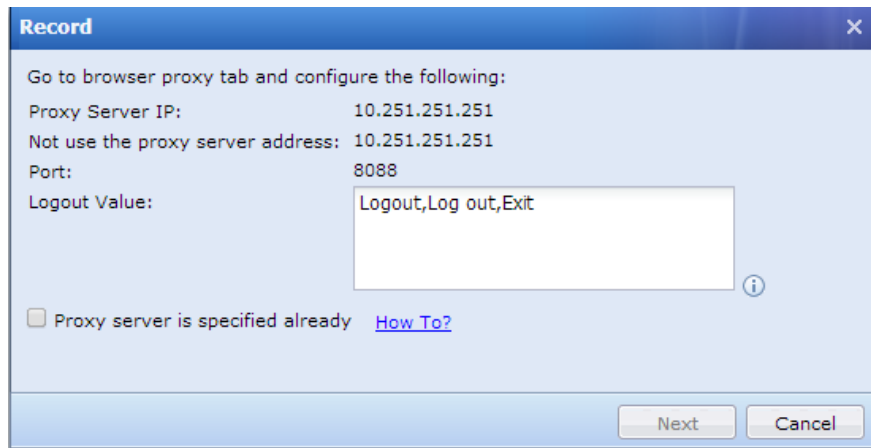
Start URL : It defines the initial directory of the website that the scanning start with.

Click on  to open the site setting page as shown below:



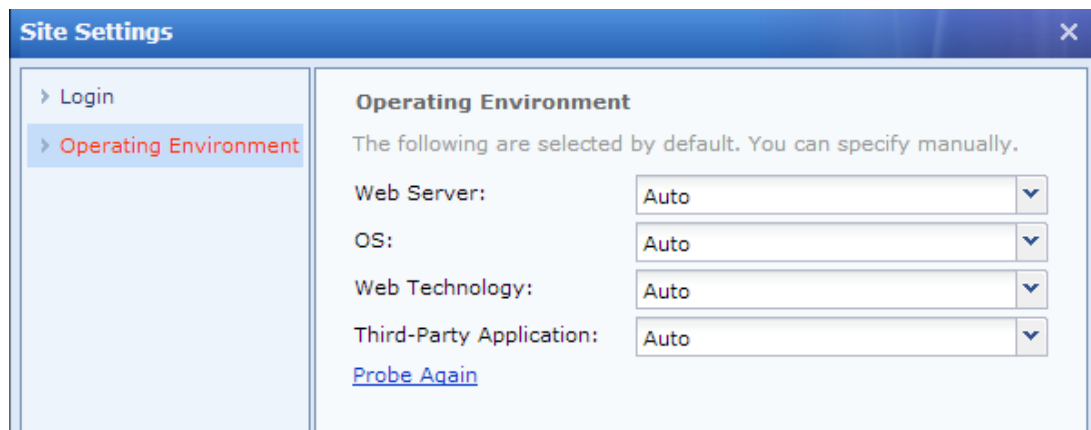
Login : Select **No need to log in** for website which does not require authentication and select **Remember login credential** for website which require authentication.

If the website require authentication and after selected **Remember login credential**, Click on  to open **Record** page. See the following figure:



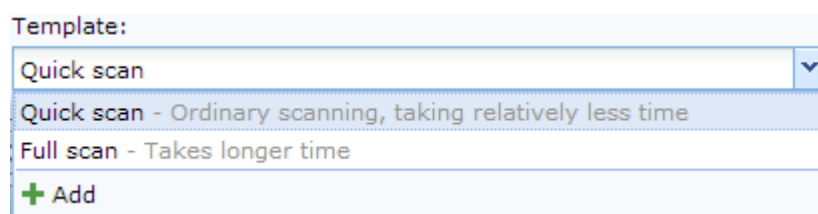
Follow the instructions in the wizard and save the record under the **Remember login credential** and the record can be used in the next scanning. Configure the possible keywords shown on the page after login successfully in the **Logout Value** column and if the any of the keywords in **Logout Value** column match with the keyword, the login will be thought as succeeded and the login credential will be remembered.

Operating Environment : Use for determine Web Server type, OS type, Web Technology used, and third-party Application type manually. The settings are set to **Auto** by default. Refer to the figure below:

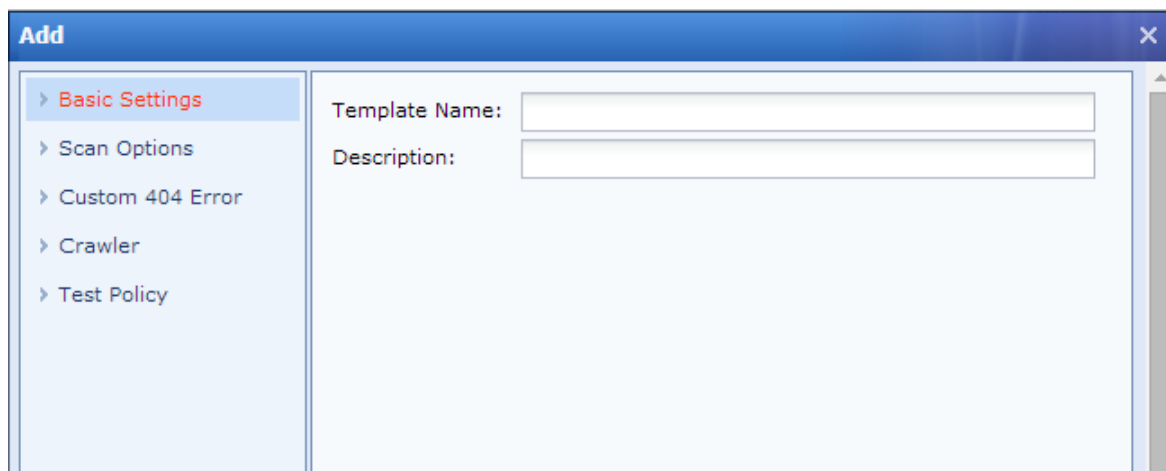


Click on **Probe Again** to examine and explore the Operating Environment of the Website.

Template : Templates are used to determine the scanning contents and scanning options which will be discuss in the section later. By default, there are two templates available, naming **Quick scan** and **Full scan**. Additional templates can be added in order to fulfill user's requirement.



Click on **Add** and the following page will be shown:

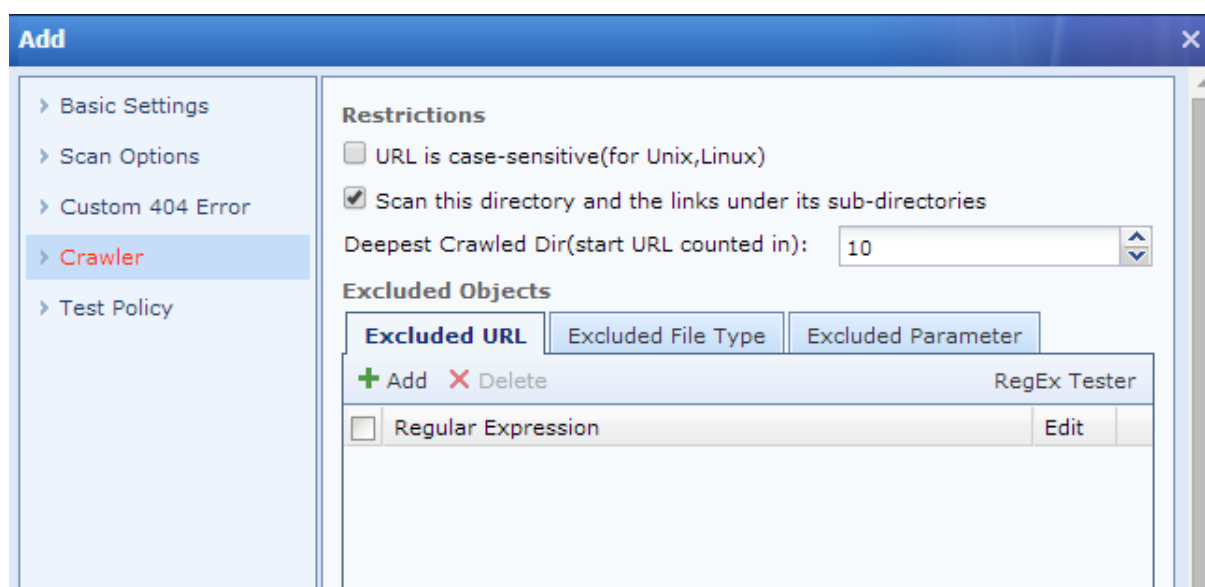


Basic Settings : To define Name and Description for the new template.


Scan Options : To define Scanning Restriction such as Request Timeout in seconds, Max Attempts, Max threads, Longest Scanning in minutes, Max File Size for Scan in byte(s) and Enhance Scanning option. Configuration for Proxy Server and port fall under this page as well.


Custom 404 Error : To add Regular Expression and if the regular expression match with the website page, it is recognized as custom 404 error page. This helps to provide more correct scanning results. **RegEx Tester** is available on the page.

Crawler : To define Restrictions such as URL's case-sensitivity(for Unix, Linux), directory and the link under its sub-directories to be scan and the deepest crawled Directory. Other configurations such as Excluded URL, Excluded File Type and Excluded Parameter are found on this page. See the figure below:

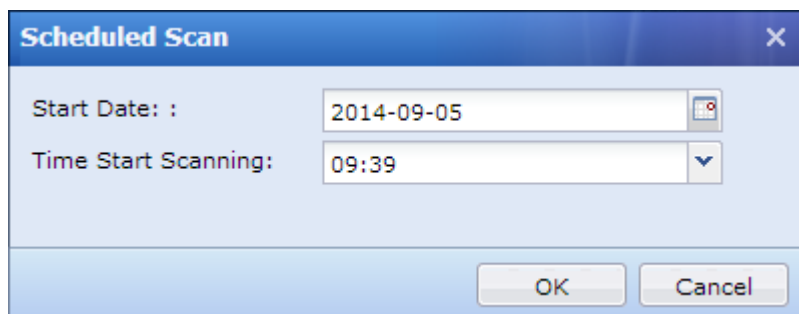




Test Policy : To determine the policy used to do web scanning for this template.










After the **Start URL** and **Template** have been configured, click on  button to initiate the web scanning and after a while the results will be displayed.


Click on  to configure the date and time for scanning on the scheduled scan page, refer

to the following figure :

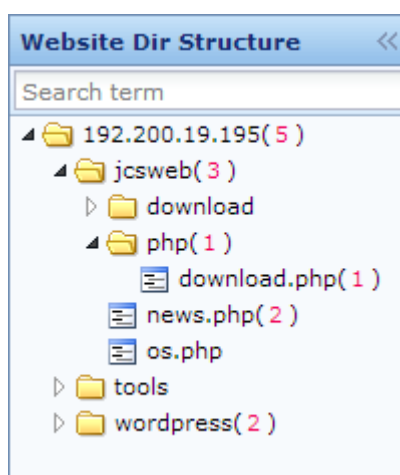



Click on [Scan History](#) to show the previous scans done. Click on  to re-scan the web server and  to delete the scan history. See the following figure :

Scan History					
 Delete					
<input type="checkbox"/>	No.	Start URL	Last Scan	Re-Scan	Delete
<input type="checkbox"/>	1	http://192.200.19.195/jcsweb	2014-09-04 18:01:19 - 18:03:49		
<input type="checkbox"/>	2	http://192.200.19.195/	2014-09-04 17:15:03 - 17:17:57		
<input type="checkbox"/>	3	http://192.200.19.200/	2014-09-04 16:55:56 - 16:55:56		
<input type="checkbox"/>	4	http://192.200.200.33/	2014-09-04 15:52:21 - 15:52:59		

Click  **Export Report as HTML File** to download the scan results in HTML file type.

Web Dir Structure shows the directory structure of the scan website and the pages which contain the vulnerability. Refer to the figure below:



The results table contains two fields: **Vulnerability** and **Threat Level**. Click on the  to expand the **Process**, **Description** and **Recommended Solution** fields.

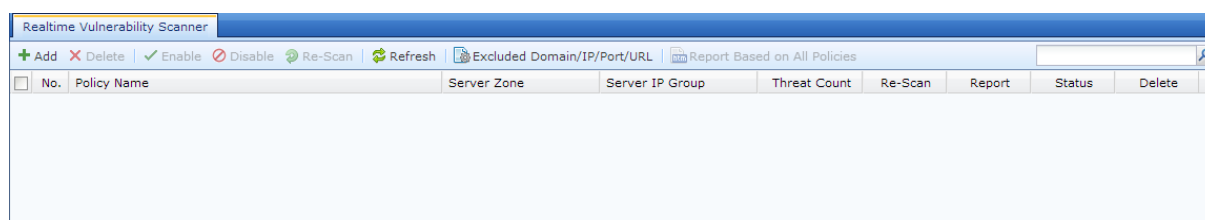
The scan results page is shown as below:




Click on  to go back to the scan page.

RT Vulnerability Scanner

Realtime Vulnerability Scanner scans the real time vulnerabilities available on the server based on the vulnerability rules placed under the **Security Database**. The scan result shows the number of threat count found on the server and more details such as threat information, threat level and suggested solutions can be found in the report. Server Administrator can defense against the vulnerabilities and take actions accordingly by refer to the report. See the following figure:



Click  to add and configure a new policy to perform RT vulnerability scanning on targeted server. The following page will be shown:

The screenshot shows the 'Add' dialog box. It has a title bar with 'Add' and a close button. Inside, there is a checkbox labeled 'Enable' which is checked. Below it are four input fields: 'Policy Name:', 'Description:', 'Server Zone:', and 'Server IP Group:'. The 'Server Zone' and 'Server IP Group' fields have a 'Select' button next to them. At the bottom, there are three buttons: 'Save and Add', 'OK', and 'Cancel'.


Policy Name: To define the name for the new policy.

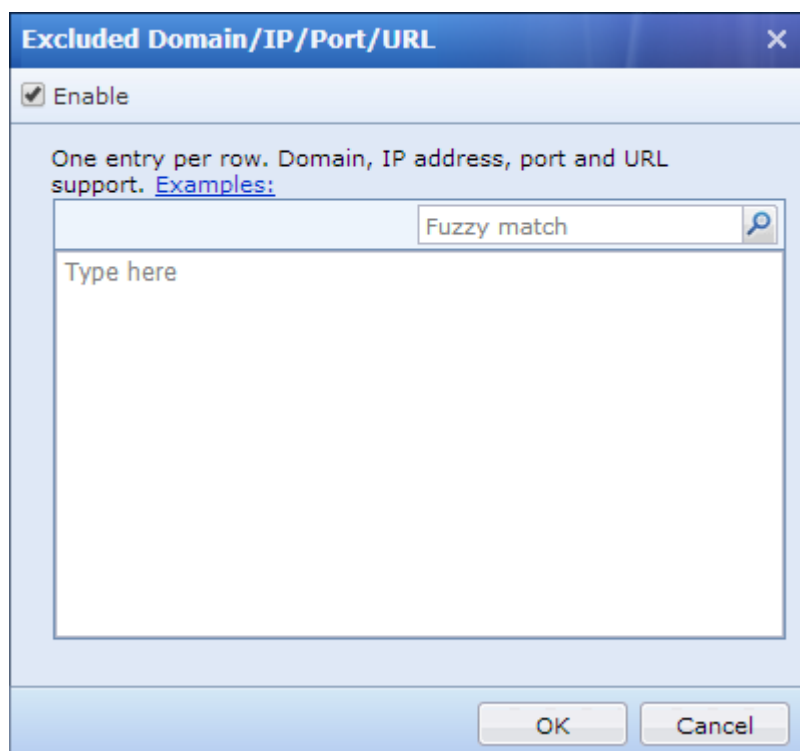
Server Zone: To select the Zone which the server located.

Server IP Group: To select the IP Group of the server(s) which need to perform RT Vulnerability Scan test on.

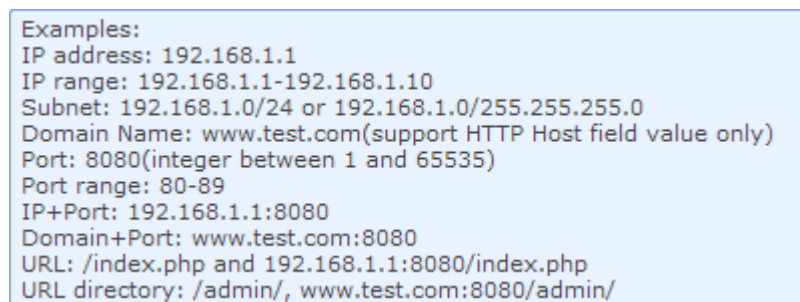
Click  **Re-Scan** or [Re-Scan](#) to re-attempt to perform the related scanning policy.


Click  **Refresh** to get the latest scanning result of all policies.

Click  **Excluded Domain/IP/Port/URL** to open the page for excluded domain, IP address, port and URL configuration. See the figure below:



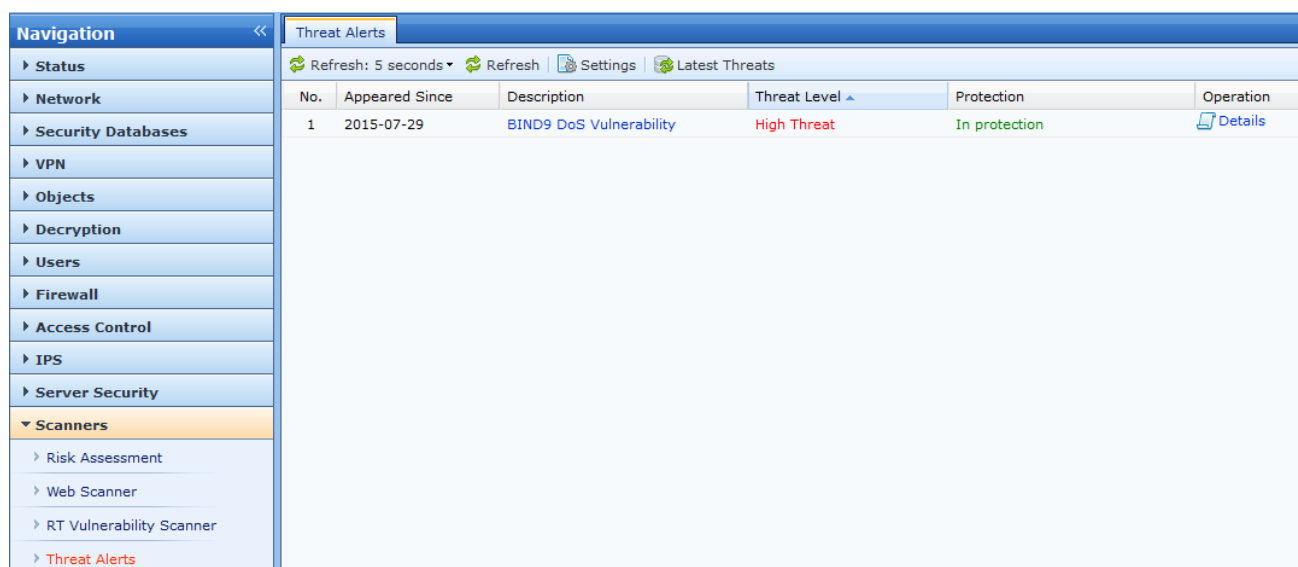
Select the [Examples:](#) to show the supported format of Domain, IP address, Port and URL. Refer to the following figure:



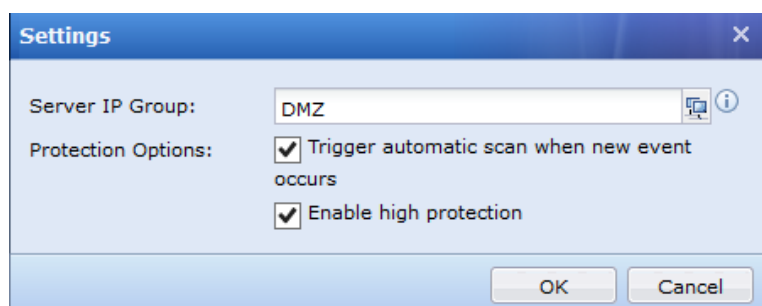
Click on  **Report Based on All Policies** to generate a report in HTML format which contains the scan results of all the policies configured.

Threat Alerts

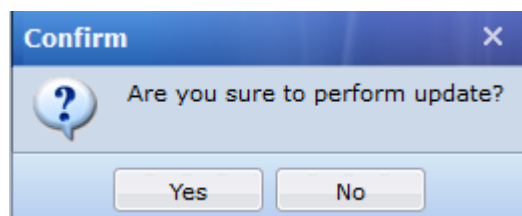
This Threat Alerts is used to display or alert any new threats around the world. If your network is vulnerable to the new threats, NGAF will alert you to take action in order to protect the network security.



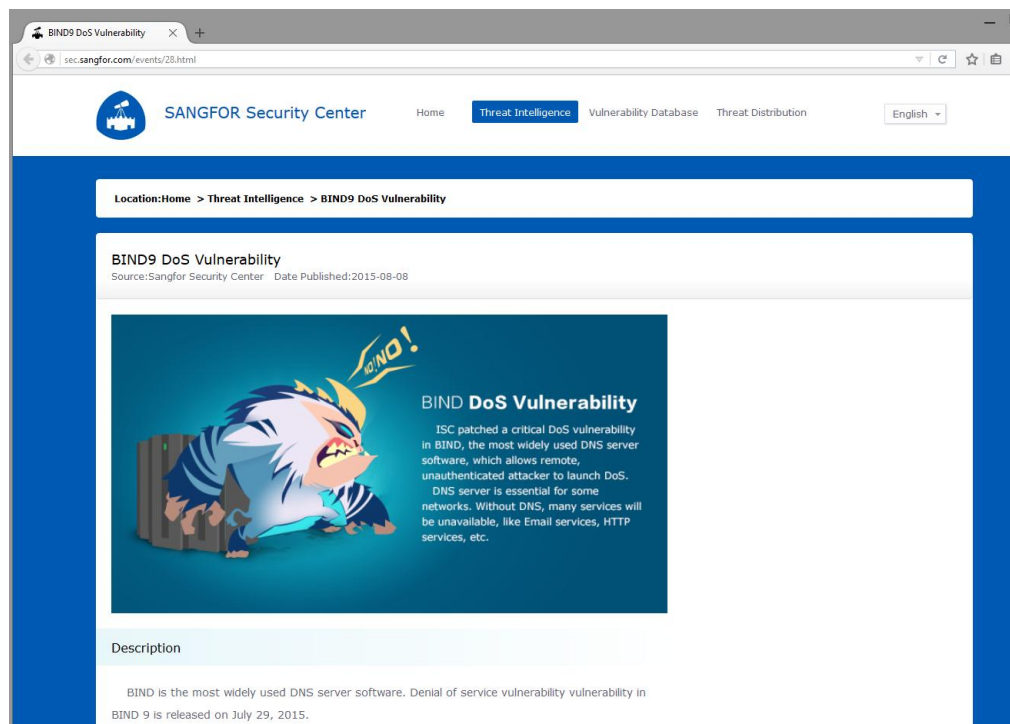
Click **Scanners > Threat Alerts > Settings** to add in the Server IP Group with the threat scan and alert functions. Below is the sample of DMZ IP Group with protection options.



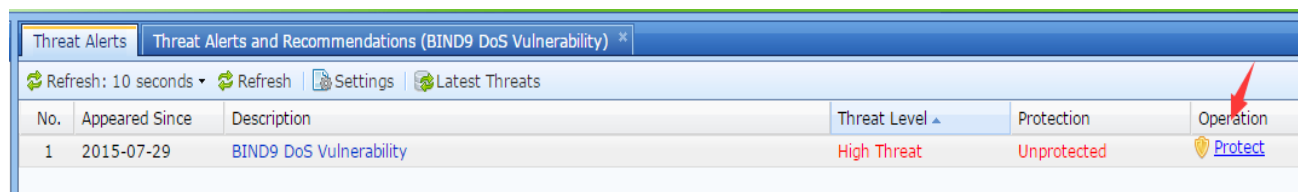
Click **Scanner > Threat Alerts > Latest Threats** to update the threat library and threat status of protected device.



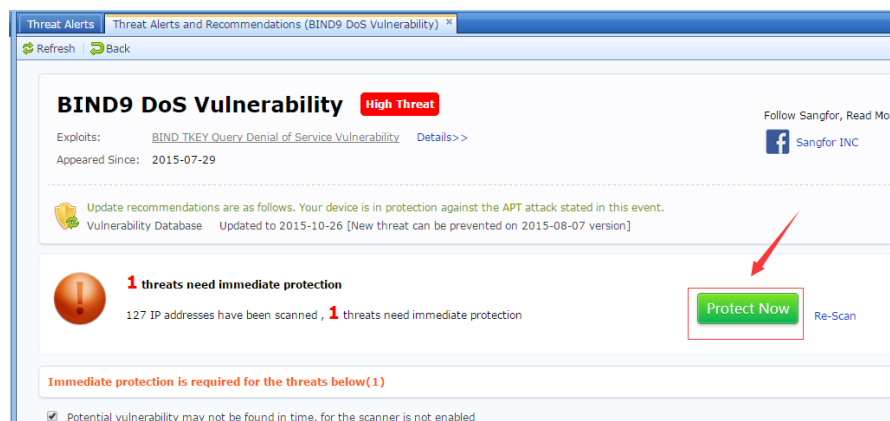
For more information about the threat, you can select the **Name of Threat** under the **Description** column. It will open a website about the clicked threat. See the figure below.



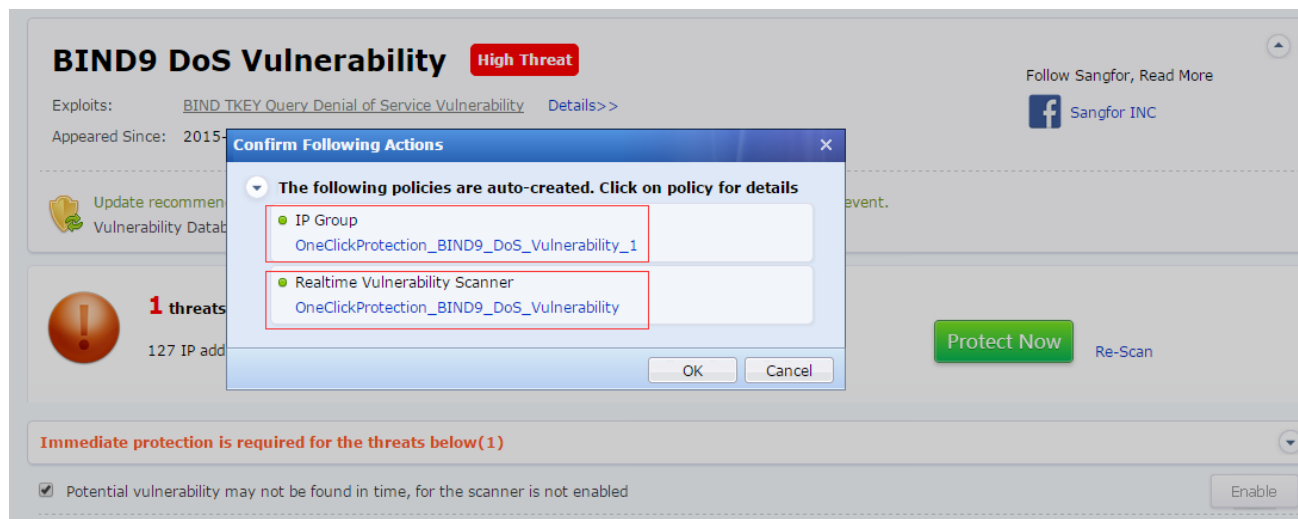
There are a few steps to protect the server from threats. Click **Protect** under the **Operation** column. See the figure below.



It will open up another tab, click **Protect Now** to perform the protection. See the figure below

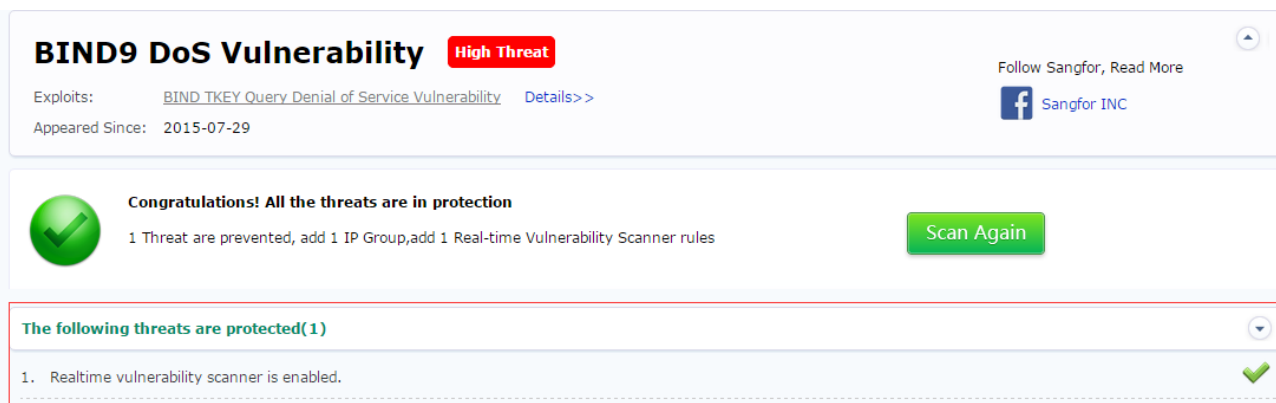


NGAF will ask confirmation to add these **new policies** to protect from the threats. Click **OK** to implement. See the figure below.



The threat is prevented successfully with the result.

Scan Again button is used to scan all the Server IP Group again which defined by user. See the figure below.



Traffic Management

Overview

The traffic management function controls the traffic size of various Internet accessing applications by establishing traffic management channels.

The NGAF offers the bandwidth guarantee and restriction functions. The bandwidth guarantee function helps to provide assured bandwidth to important applications, while the bandwidth restriction function helps to restrict the total uplink and downlink bandwidth of users or user groups and bandwidth occupied by various applications.

The traffic management function provides the traffic sub-channel function. You can set up traffic sub-channels as required to distribute channel bandwidth in a refined way.

Basic concepts:

Traffic channel: The total bandwidth is divided into several parts in percentage as traffic channels for different service types and access control user groups. The traffic channels are grouped into traffic guarantee channels and traffic restriction channels by function.

Traffic restriction channel: The maximum data speed is defined for the channel. When the network is busy, the bandwidth occupied by the channel does not exceed the maximum bandwidth specified for the channel.

Bandwidth guarantee channel: The channel is configured with a maximum bandwidth and a minimum bandwidth. When the network is busy, the bandwidth available to the channel is no smaller than the minimum bandwidth specified for the channel.

BM line: The BM line maps the physical network interface to the effective line of a traffic channel, to specify which interface matches a traffic channel in dataflow.

Traffic Channel Mapping and Priority

When the traffic management function is enabled, the NGAF maps the dataflow to the traffic channel based on the user group/user, IP address, application type, effective time, and destination IP group. Only when all the above information in the data packet matches the condition of a traffic channel, the traffic channel is applied to the data packets.

Same data packets are mapped to one traffic control policy. The NGAF verifies traffic control policies from top to bottom one by one. Therefore, traffic channels with more specific conditions must be located on the top.

Channel Configuration

Traffic Guarantee Channel

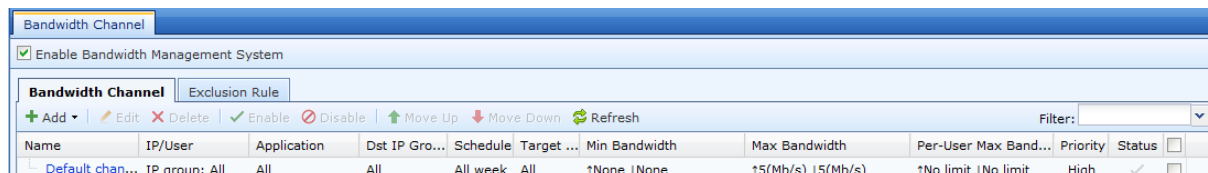
To provide important applications with assured bandwidth when the network is busy, you can set minimum bandwidth for specific types of data packets.

3.12.7.1.1 Configuring Traffic Guarantee Channel

Example: Assume that a company has rented a 10 Mb/s telecom data line, has 1000 users accessing the Internet, and needs to ensure that the financial department enjoys the bandwidth from 2 Mb/s to 5 Mb/s for visiting online banks and receiving and sending emails when the network is busy.

Step 1 Choose **Traffic Management > Bandwidth Channel**.

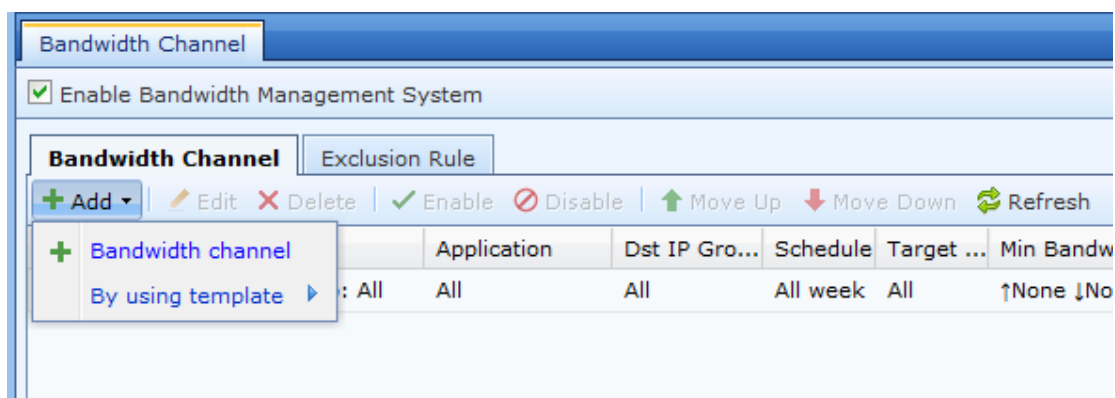
Select **Enable Bandwidth Management System**.



Step 2 Choose **Traffic Management > BM Line** and set the BM line list and policy. For details, see section 3.12.4.

Step 3 Configure the traffic guarantee channel.

In this example, the assured network bandwidth is provided to the financial department for visiting online banks and receiving and sending emails when the network is busy.



On the **Bandwidth Channel** tab page, click **Add** and choose **Bandwidth channel**. The **Add Bandwidth Channel** screen is displayed.

Add Bandwidth Channel

☒ Enable channel

Name:

Options

- > **Bandwidth Channel**
- > Applicable Objects

Bandwidth Channel

Target Line:

Channel Type

☒ **Guaranteed channel**

Outbound: Min % Mbps

Max % Mbps

Inbound: Min % Mbps

Max % Mbps

Priority:

☐ **Limited channel**

Outbound: Max % Mbps

Inbound: Max % Mbps

Priority:

☐ **Per-User Max Bandwidth**

OK Cancel

Select **Enable channel**. If the checkbox is deselected, the traffic control function of the channel does not take effect.

Enter the channel name in **Name**.

Choose **Bandwidth Channel** under **Options**. Set the properties of the channel on the right.

Add Bandwidth Channel

☒ Enable channel

Name:

Options

- Bandwidth Channel
- Applicable Objects

Bandwidth Channel

Target Line:

Channel Type

☒ **Guaranteed channel**

Outbound: Min % Kbps Max % Kbps

Inbound: Min % Kbps Max % Kbps

Priority:

☐ **Limited channel**

Outbound: Max % Mbps

Inbound: Max % Mbps

Priority:

☐ **Per-User Max Bandwidth**

OK Cancel

The menu **Bandwidth Channel** under **Options** is used to set the target line, channel type, restricted or guaranteed bandwidth, and bandwidth per user.

The parameter **Target Line** defines the applicable line of the channel. That is, only the data packets on the specified line are mapped to the channel. The lines listed in the list box of **Target Line** are specified in **BM Line** in advance. For details about how to set up BM lines, see section 3.12.4.

The **Channel Type** area is where the channel type and bandwidth range are defined. In this example, the financial department is guaranteed with the bandwidth from 2 Mb/s to 5 Mb/s for visiting online banks and receiving and sending emails. Thus, select **Guaranteed channel**. Set **Min** and **Max** of **Outbound** and **Inbound** to **20%** and **50%** respectively. The total bandwidth is 10 Mb/s. Therefore, the minimum bandwidth will be 2 Mb/s and the maximum bandwidth will be 5 Mb/s. The **Priority** can be set to **High**, **Medium**, and **Low**, indicating the priority of the channel occupying other available channels.

☐ **Per-User Max Bandwidth**

Outbound: Kbps ▼

Inbound: Kbps ▼

Advanced

☐ Make allocated bandwidth on this bandwidth channel shared evenly among external IP addresses and Per-User Max Bandwidth setting applied to each of them (typically selected for server providing external services)

The parameter **Per-User Max Bandwidth** is used to set the bandwidth each IP address in the channel can enjoy. In this example, the parameter is left empty.

If you select **Evenly allocation** for **Bandwidth Allocation Among Users**, the bandwidth is allocated evenly among the users in the channel. Here, the users indicate those who have dataflow mapped to the channel. Users within the scope of the channel but do not send or receive dataflow over the channel are not involved. **Free competition** is not available.

If you select **Make allocated bandwidth on this bandwidth shared evenly among...**, each user of an external IP address is taken as a user of the channel and the bandwidth allocation policy among users and per-user bandwidth configuration are effective to external IP addresses. (Be cautious. This option is usually applied to the servers providing services on the Internet.)

The menu **Applicable Objects** under **Options** is used to define what types of data packets are mapped to the channel, in terms of application type, applicable objects, effective time, object IP group, sub-interface, and VLAN. The channel is applicable only when all the conditions are met.

Add Bandwidth Channel

☒ Enable channel

Name:

Options

- > Bandwidth Channel
- > **Applicable Objects**

Applicable Objects

Application: ☒ All
☐ Specified
[Select Application](#)

IP/User: ☒ IP Group

☐ User

Schedule:

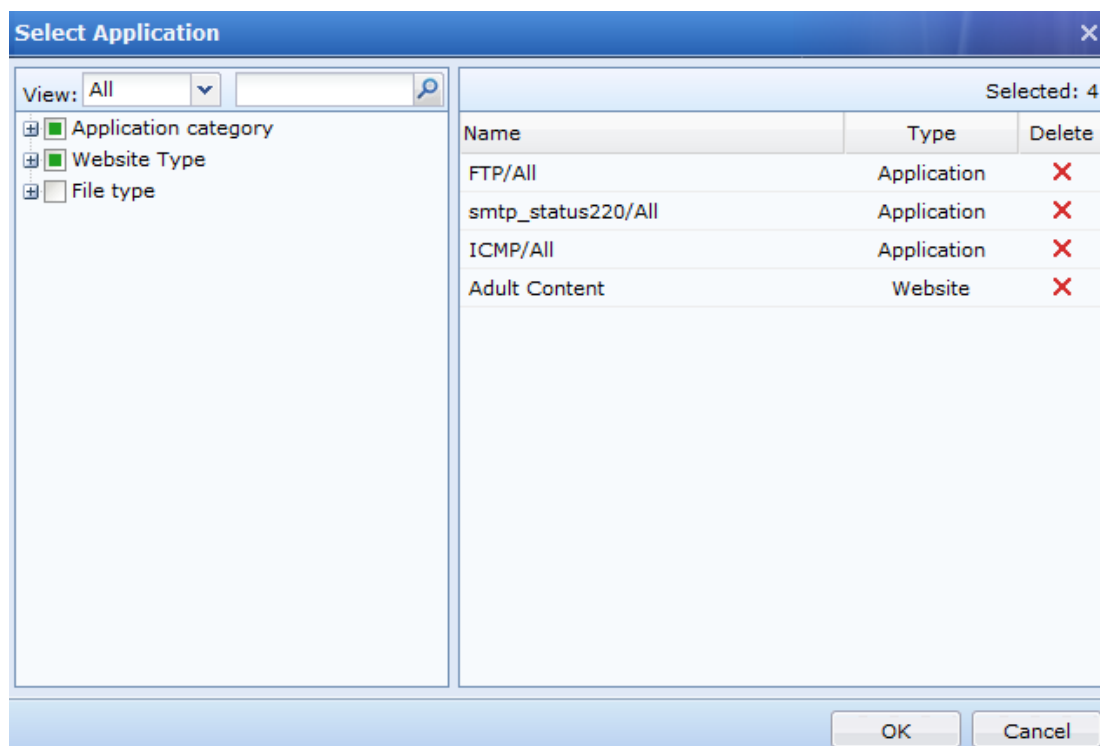
Dst IP Group:

☒ Sub-Interface

☐ VLAN [i](#)

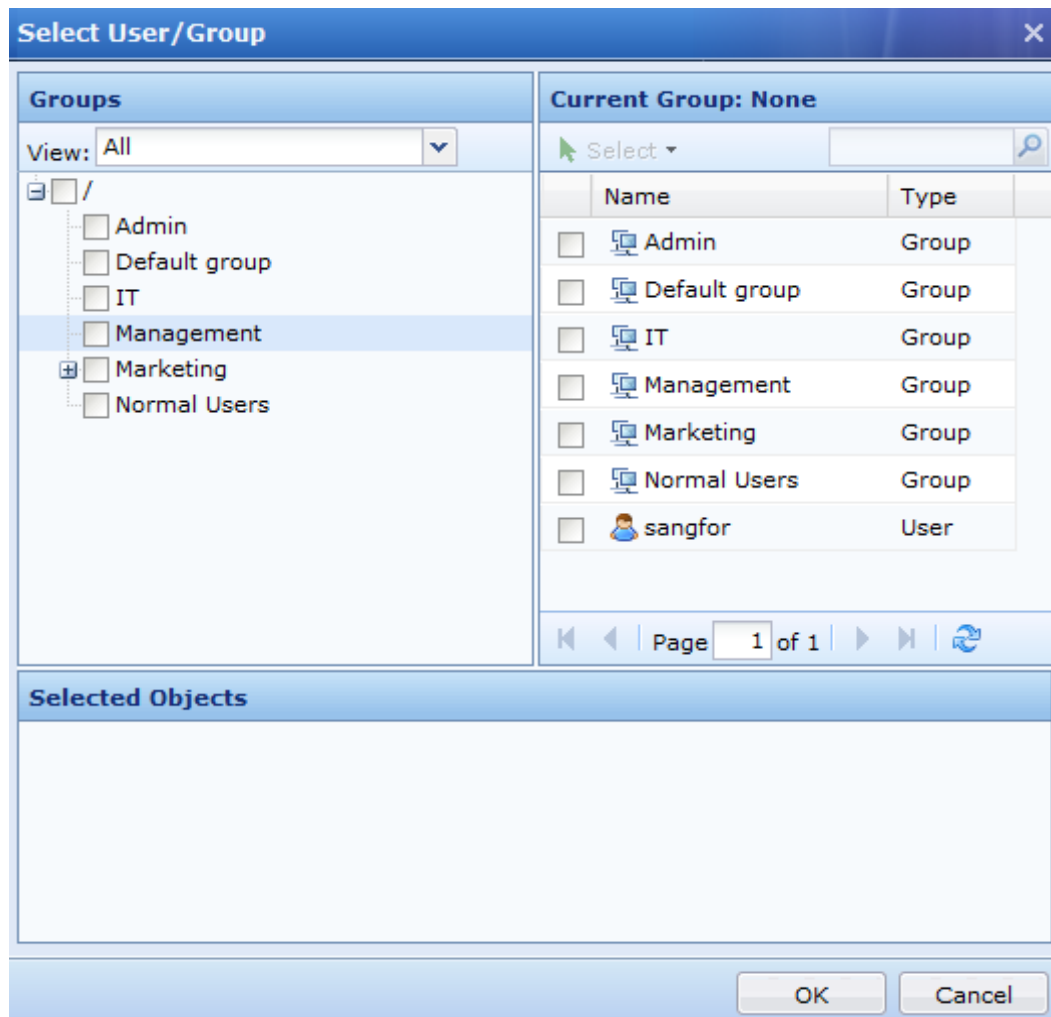
OK Cancel

Application defines the application type. You can select **All** to apply the channel to the data packets of all types of applications, and **Specified** to apply the channel to data packets of specific applications. Click **Select Application**. In the displayed screen, select **Application category** and **Website Type**. In this example, services mail receiving and sending and online bank visiting are guaranteed with bandwidth. Therefore, select **Email/All** for **Application category** and **Online bank** for **Website Type**.



The **File type** category controls the download of files over HTTP and FTP. In the **Selected** list, check that all selected objects are correct, and click **OK**.

The configuration of **Applicable Objects** defines the channel takes effect for which users, user groups, and IP addresses based on IP addresses or users. In this example, the users in the financial department are provided with guaranteed bandwidth. Therefore, choose **User** for **IP/User**, and select the group in the displayed **Select User/Group** screen. You can select users and user groups under **Current Group**. The selected users and user groups are listed under **Selected Objects**. After all required objects are selected, click **OK**. The configuration is complete.



Schedule defines the effective time of the channel.

Dst IP Group defines the destination IP address groups of the channel.

Sub-Interface defines to set the sub-interface of the channel.

VLAN defines the applicable VLAN of the channel.

The complete configuration is shown in the following figure:

After the configuration is complete, click **OK**.

Step 4 The configured channel is listed under **Bandwidth Channel**. The traffic guarantee channel is configured.

Name	IP/User	Application	Dst IP Gro...	Schedule	Target ...	Min Bandwidth	Max Bandwidth	Per-User Max Band...	Priority	Status
Marketing	IP group: All	All	All	All week	Line 1	↑11(Mb/s) ↓1(Mb/s)	↑11(Mb/s) ↓1(Mb/s)	↑No limit ↓No limit	High	✓
Default chan...	IP group: All	All	All	All week	All	↑None ↓None	↑5(Mb/s) ↓5(Mb/s)	↑No limit ↓No limit	High	✓



1. The total guarantee bandwidth percentage of all channels may exceed 100%. If so, the minimum bandwidth percentage of each channel is reduced in proportion. For example, if two channels are configured, with one guarantee channel percentage at 30% and the other 90%, the first channel is allocated with $30/(90+30)\%$, that is 25%, and the other being $90/(90+30)\%$, that is 75%.
2. Priority: If the actual bandwidth is not occupied fully, the channel with higher priority preempts the non-occupied bandwidth.

Traffic Restriction Channel

You can set a maximum bandwidth for a channel to restrict the bandwidth allocated to the channel. In this case, the bandwidth occupied by the channel does not exceed the maximum bandwidth.

3.12.7.2.1 Configuring Traffic Restriction Channel

Example: Assume that a company has rented a 10 Mb/s telecom data line, has 1000 users accessing the Internet, and needs to ensure normal business not be affected by Thunder Download or P2P downloading services which sales department employees use frequently. The bandwidth occupied by data downloading services of the sales department is restricted to under 2 Mb/s, with per-user bandwidth of these services under 30 Kb/s.

Step 1 Choose **Traffic Management > Channel Configuration**.

Select **Enable Bandwidth Management System**.

Step 2 Choose **Traffic Management > BM Line** and set the BM line list and policy. For details, see section 3.12.4.

Step 3 Configure the traffic restriction channel.

In this example, the P2P and download data of the sales department employees are controlled. The total bandwidth occupied by these services is restricted to below 2 Mb/s for the department.

On the **Bandwidth Channel** tab page, click **Add** and choose **Bandwidth channel**. The **Add Bandwidth Channel** screen is displayed.

Select **Enable channel**. If the checkbox is deselected, the traffic control function of the channel does not take effect.

Enter the channel name in **Name**. The slash / before the channel indicates a primary channel.

Choose **Bandwidth Channel** under **Options**. Set the properties of the channel on the right.

Add Bandwidth Channel

☒ Enable channel

Name:

Options

- Bandwidth Channel
- Applicable Objects

Bandwidth Channel

☐ Guaranteed channel

Outbound: Min % Mbps ▾
 Max % Mbps ▾

Inbound: Min % Mbps ▾
 Max % Mbps ▾

Priority: ▾

☒ Limited channel

Outbound: Max % Kbps ▾

Inbound: Max % Kbps ▾

Priority: ▾

☐ Per-User Max Bandwidth

Outbound: Kbps ▾

Inbound: Kbps ▾

OK Cancel

The menu **Bandwidth Channel** under **Options** is used to set the effective line, channel type, restricted or guaranteed bandwidth, and bandwidth per user.

The parameter **Target Line** defines the applicable line of the channel. That is, only the data packets on the specified line are mapped to the channel. For details about how to set up target lines, see section 3.12.4.

The **Channel Type** area is where the channel type and bandwidth range are defined. In this example, the bandwidth for the P2P and data download services of the sales department is restricted. Thus, select **Limited channel**. Set **Outbound** and **Inbound** to **20%** respectively. The total bandwidth is 10 Mb/s. Therefore, the maximum bandwidth will be 2 Mb/s. The **Priority** can be set to **High**, **Medium**, and **Low**, indicating the preemption priority of the channel occupying other available channels.

Add Bandwidth Channel

☒ Enable channel

Name:

Options

- > **Bandwidth Channel**
- > Applicable Objects

Bandwidth Channel

☒ Limited channel

Outbound: Max % Kbps ▾

Inbound: Max % Kbps ▾

Priority: ▾

☒ **Per-User Max Bandwidth**

Outbound: Kbps ▾

Inbound: Kbps ▾

Advanced

☐ Make allocated bandwidth on this bandwidth channel shared evenly among external IP addresses and Per-User Max Bandwidth setting applied to each of them (typically selected for server providing external services)

OK Cancel

The parameter **Per-User Max Bandwidth** is used to set the bandwidth each IP address in the channel can enjoy. In this example, enter 30 Kb/s for **Outbound** and **Inbound**.

If you select **Even allocation** for **Bandwidth Allocation Among Users**, the bandwidth is allocated evenly among the users in the channel. Here, the users indicate those who have dataflow mapped to the channel. Users within the scope of the channel but do not send or receive dataflow over the channel are not involved. **Free competition** is not available.

If you select **Make allocated bandwidth on this bandwidth shared evenly among...**, each user of an external IP address is taken as a user of the channel and the bandwidth allocation policy among users and per-user bandwidth configuration are effective to external IP addresses. (Be cautious. This option is usually applied to the servers providing services on the Internet.)

The menu **Applicable Objects** under **Options** is used to define what types of data packets are mapped to the channel, in terms of application type, applicable objects, effective time, object IP group, sub-interface, and VLAN. The channel is applicable only when all the conditions are met.

Add Bandwidth Channel

☒ Enable channel

Name:

Options

- Bandwidth Channel
- Applicable Objects**

Applicable Objects

Application: ☒ All
☐ Specified
[Select Application](#)

IP/User: ☒ IP Group

☐ User

Schedule:

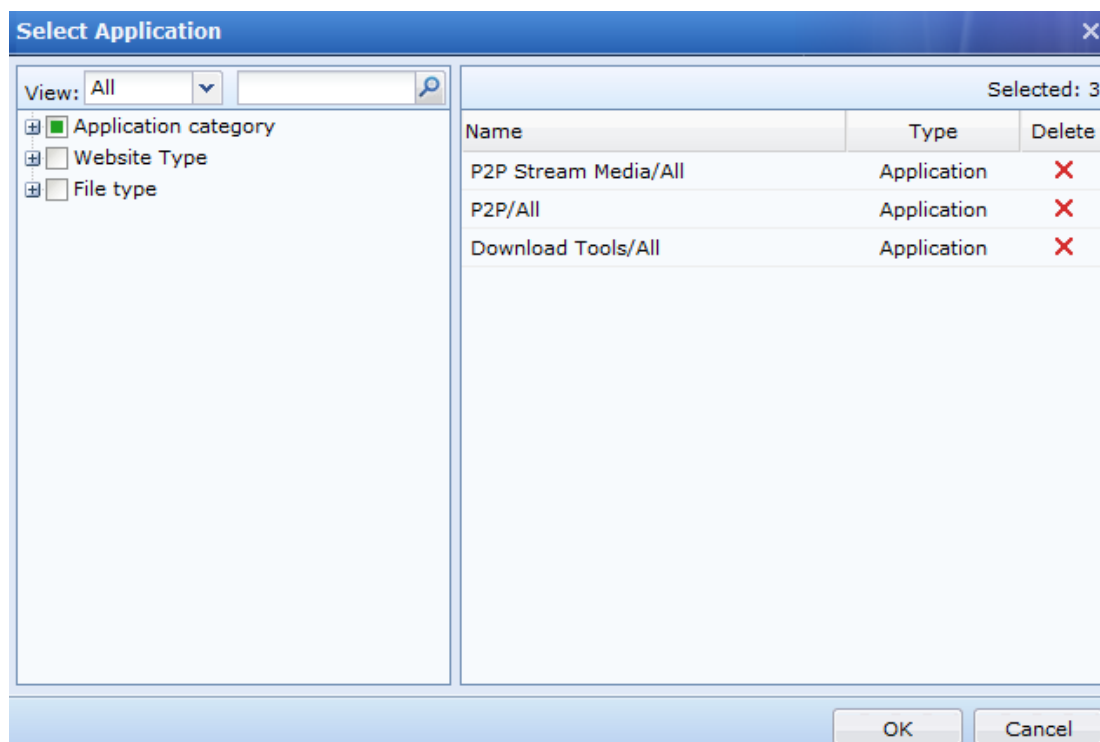
Dst IP Group:

☒ Sub-Interface

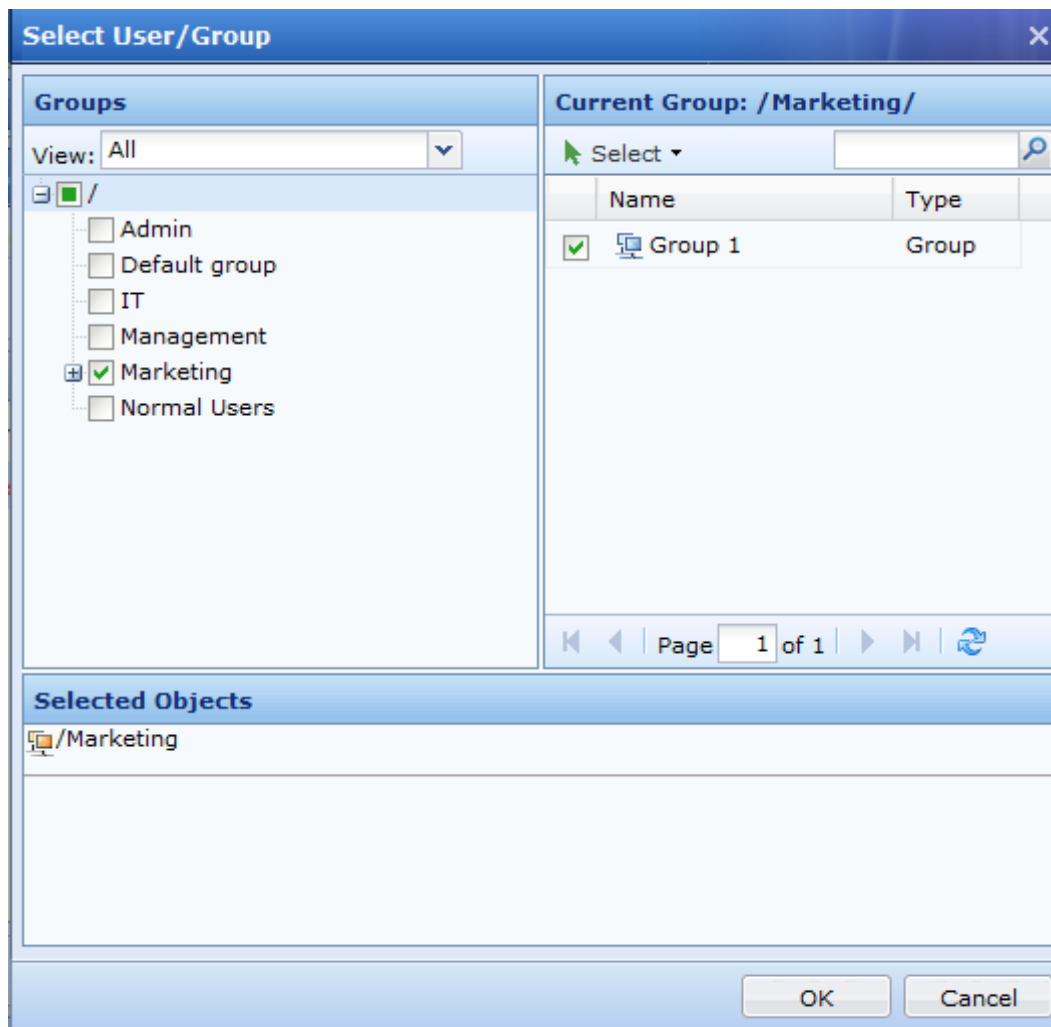
☐ VLAN [i](#)

OK Cancel

Application defines the application type. You can select **All** to apply the channel to the data packets of all types of applications, and **Specified** to apply the channel to data packets of specific applications. Click **Select Application**. In the displayed screen, select **Application category**. In this example, P2P and downloading applications are restricted in bandwidth. Therefore, select **P2P Stream Media/All**, **Download Tools/All**, and **P2P/All** for **Application category**. You can also select **Website Type** and **File type** to restrict the bandwidth for accessing certain Websites or for downloading certain types of files over HTTP and FTP. In the **Selected** list, check that all selected objects are correct, and click **OK**.



The configuration of **Applicable Objects** defines the channel takes effect for which users, user groups, and IP addresses based on IP addresses or users. In this example, employees of the sales department are applied with this bandwidth restriction configuration. Therefore, choose **User** for **IP/User**, and select the group in the displayed **Select User/Group** screen. You can select users and user groups under **Current Group**. The selected users and user groups are listed under **Selected Objects**. After all required objects are selected, click **OK**. The configuration is complete.



Schedule defines the effective time of the channel.

Dst IP Group defines the destination IP address groups of the channel.

Sub-Interface is used to set the sub-interface of the channel.

VLAN defines the applicable VLAN of the channel.

The complete configuration is shown in the following figure:

After the configuration is complete, click **OK**.

Step 4 The configured channel is listed under **Bandwidth Channel**. The traffic restriction channel is configured.

Name	IP/User	Application	Dst IP Group	Schedule	Target	Min Bandwidth	Max Bandwidth	Per-User Max Bandwidth	Priority	Status
P2P limit	User group: /...	P2P Stream M...	All	All week	Line 1	↑None ↓None	↑4(Mb/s) ↓4(Mb/s)	↑120(Kb/s) ↓120(K...	Low	✓
Marketing	IP group: All	All	All	All week	Line 1	↑1(Mb/s) ↓1(Mb/s)	↑1(Mb/s) ↓1(Mb/s)	↑No limit ↓No limit	High	✓
Default chan...	IP group: All	All	All	All week	All	↑None ↓None	↑5(Mb/s) ↓5(Mb/s)	↑No limit ↓No limit	High	✓

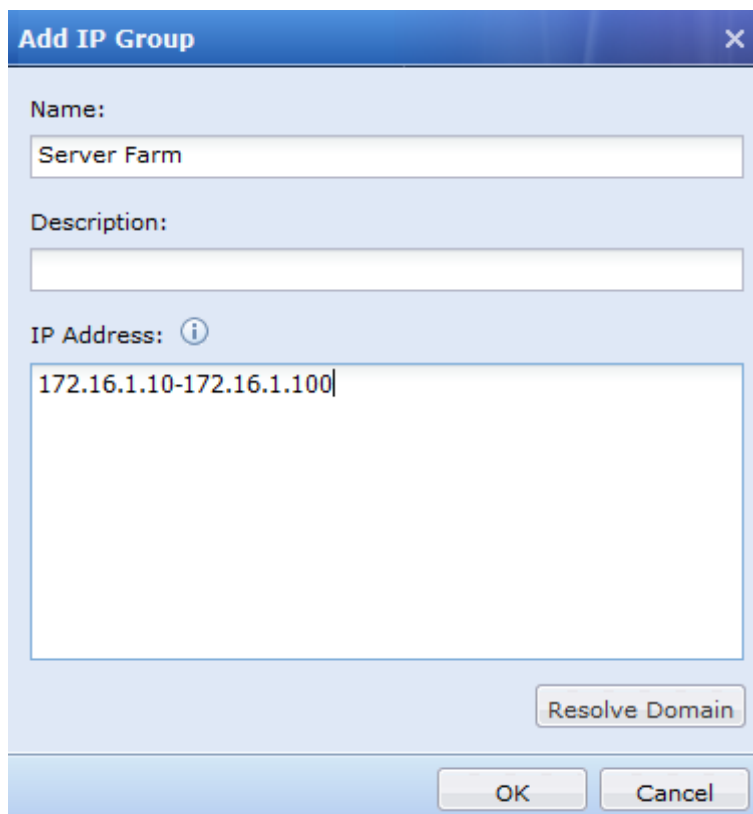
Exclusion Rule

The exclusion rule is used to define the data types that are not applicable to any traffic management channels. The exclusion rule helps involved types of dataflow not be affected by traffic management policies, for example, the dataflow from the Intranet accessing the servers deployed on the DMZ of a front firewall, with the NGAF deployed in bridge mode. As these data packets do not pass through the Internet, these data packets shall not be restricted to the bandwidth restriction policies of the Internet, and applications or IP addresses involved with those servers shall be added to exclusion rules.

3.12.7.3.1 User Configuration

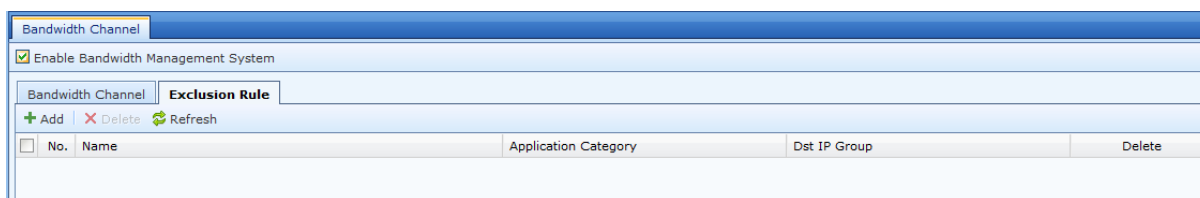
Example: Assume that the NGAF is deployed in bridge mode, servers are deployed on the DMZ of the front firewall, and an exclusion rule is to be configured for the dataflow accessing these servers.

Step 1 Choose **Object Define > IP Group**. Click **Add**. On the displayed screen, enter the IP address that applies to the exclusion rule.



The 'Add IP Group' dialog box has a blue header with the title 'Add IP Group' and a close button. It contains three input fields: 'Name' with the text 'Server Farm', 'Description' which is empty, and 'IP Address' with the text '172.16.1.10-172.16.1.100'. An information icon is next to the 'IP Address' label. A 'Resolve Domain' button is located below the 'IP Address' field. At the bottom are 'OK' and 'Cancel' buttons.

Step 2 . Choose **Traffic Management > Channel Configuration > Exclusion Rule**. Click **Add**.

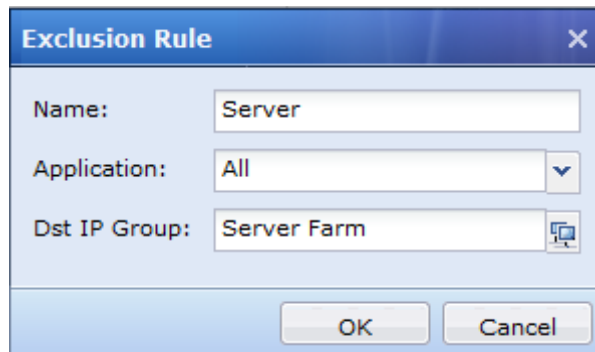


The 'Exclusion Rule' configuration window has a blue header with 'Bandwidth Channel' and 'Exclusion Rule' tabs. Below the tabs is a checkbox for 'Enable Bandwidth Management System' which is checked. Under the 'Exclusion Rule' tab, there are buttons for '+ Add', '- Delete', and 'Refresh'. Below these is a table with columns: 'No.', 'Name', 'Application Category', 'Dst IP Group', and 'Delete'.

No.	Name	Application Category	Dst IP Group	Delete
-----	------	----------------------	--------------	--------

Step 3 Set the exclusion rule.

Enter the rule name, and select the application type and destination IP group. If the application type is not fixed, select **All**. In this example, choose **Server** for **Dst IP Group**.



Exclusion Rule

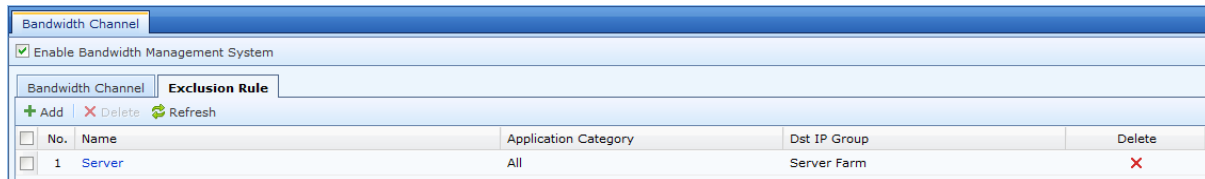
Name:

Application:

Dst IP Group:

OK Cancel

Step 4 Click **Submit**.



Bandwidth Channel

☒ Enable Bandwidth Management System

Bandwidth Channel Exclusion Rule

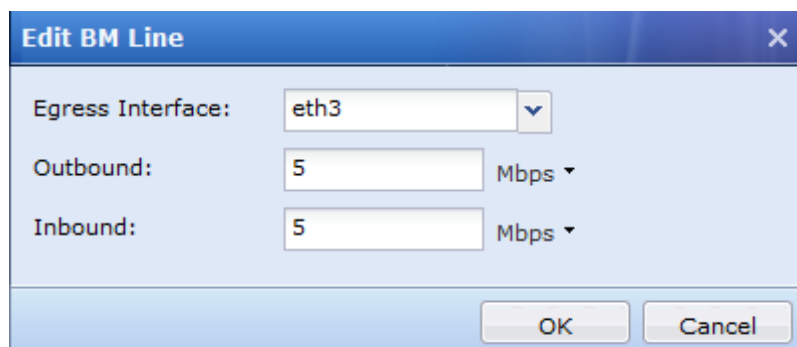
+ Add - Delete Refresh

No.	Name	Application Category	Dst IP Group	Delete
1	Server	All	Server Farm	X

BM Lines

BM Line List

The BM line list shows all the current BM lines. The BM line maps the physical network interface to the effective line of a traffic channel, to specify which egress interface (effective line) matches a traffic channel in dataflow. Click **Add**. The **Edit BM Line** screen is displayed. Set as follows:



Edit BM Line

Egress Interface:

Outbound: Mbps

Inbound: Mbps

OK Cancel

Egress Interface: defines the source interface of dataflow that is applied with the BM line. Only WAN interfaces are available.

Outbound: The outbound bandwidth of the physical line. The value must be based on the actual situation; otherwise, the traffic control effect may be poor.

Inbound: The inbound bandwidth of the physical line. The value must be based on the actual situation; otherwise, the traffic control effect may be poor.

If traffic control must be set for multiple egress interfaces, define multiple BM lines. Click **Add** to add other BM lines one by one.



After the BM lines are defined, set corresponding BM line policies with the defined lines; otherwise, the traffic control channel does not take effect.

BM Line Policy

The BM line policy is mandatory for the traffic control channels to take effect. You can define different BM line policies with different network protocols, Intranet zones, Internet zones, and outbound interfaces.

Choose **Traffic Management > BM Line > Policy**. Click **Add**. On the displayed **Add BM Line Policy** screen, set the parameters as follows:

The screenshot shows the 'Add BM Line Policy' configuration window. It has a blue header bar with the title 'Add BM Line Policy'. Below the header, there are two main sections: 'Transfer Protocol' and 'Internal Address'. In the 'Transfer Protocol' section, there is a 'Type:' label followed by a dropdown menu set to 'All', and a 'Protocol No.:' label followed by a text input field containing '0'. In the 'Internal Address' section, there is an 'IP Address:' label with two radio button options: 'All' (which is selected) and 'Specified' (which has an information icon). Below the 'Specified' option is a text input field. Similarly, there is a 'LAN Port:' label with two radio button options: 'All' (selected) and 'Specified', with a text input field below the 'Specified' option.

The screenshot shows a configuration window with two main sections. The top section, titled 'External Address', contains two rows. The first row is for 'IP Address', with radio buttons for 'All' (selected) and 'Specified' (with an information icon), followed by a text input field. The second row is for 'WAN Port', with radio buttons for 'All' (selected) and 'Specified', followed by a text input field. The bottom section, titled 'Internet Line', contains a single row for 'Internet Line' with a dropdown menu currently showing 'Line 1'.

Transfer Protocol defines the protocol type of the data packets.

Internal Address defines the source IP address and port No. of the data packets.

External Address defines the destination IP address and port No. of the data packets.

Internet Line defines the BM line of the data packets, that is, the egress interface of the data packets.

After a BM line is specified as the Internet line of a BM line policy, the traffic control channel takes effect for the BM line.

System

System Configuration

The general system configuration includes the configuration of the system time, network parameters, console configuration, and license.

System Time

On the **System Time** tab page, you can set the system time of SANFOR NGAF. You can change the time on the UI directly or set time synchronization schemes.

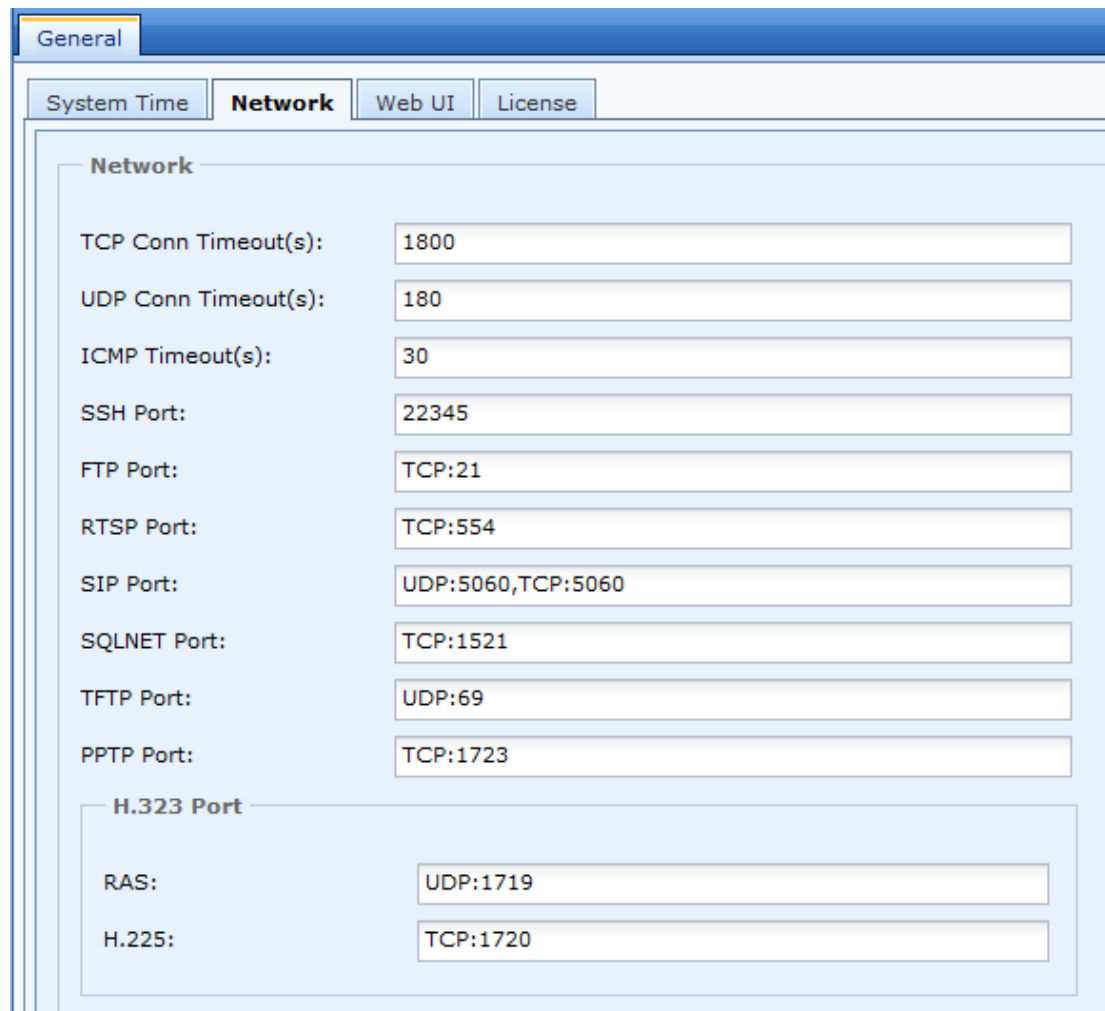
The screenshot shows a web-based configuration interface for a system. The main window is titled 'General' and contains four tabs: 'System Time', 'Network', 'Web UI', and 'License'. The 'System Time' tab is currently selected. It is divided into three sections: 'Date and Time', 'Time Zone', and 'Synchronize Time with NTP Server'. In the 'Date and Time' section, there is a 'Date' field with the value '2013-08-15' and a calendar icon, a 'System Time' field with the value '14:28:01', and two buttons: 'Sync with Local PC' and 'Restore System Time'. The 'Time Zone' section has a 'Time Zone' dropdown menu showing '(GMT+08:00) Beijing, Shanghai, Hong Kong'. The 'Synchronize Time with NTP Server' section has an 'NTP Server' field with the value 'pool.ntp.org' and a 'Sync Now' button. An 'OK' button is located at the bottom right of the window.

Under **Date and Time**, you can check the current time in the system and adjust the system time manually. You can click **Sync with Local PC** to synchronize the system time to time on the login terminal, or click **Restore System Time** to show the original time on the system.

You can also set a time synchronization scheme for the system: Select a time zone from the **Time Zone** drop-down list box and enter the NTP server address in **NTP Server**. The system automatically synchronizes time based on the specified NTP server.

Network Configuration

On the **Network** tab page, you can set the network parameters. See the following figure:



General

System Time **Network** Web UI License

Network

TCP Conn Timeout(s): 1800

UDP Conn Timeout(s): 180

ICMP Timeout(s): 30

SSH Port: 22345

FTP Port: TCP:21

RTSP Port: TCP:554

SIP Port: UDP:5060,TCP:5060

SQLNET Port: TCP:1521

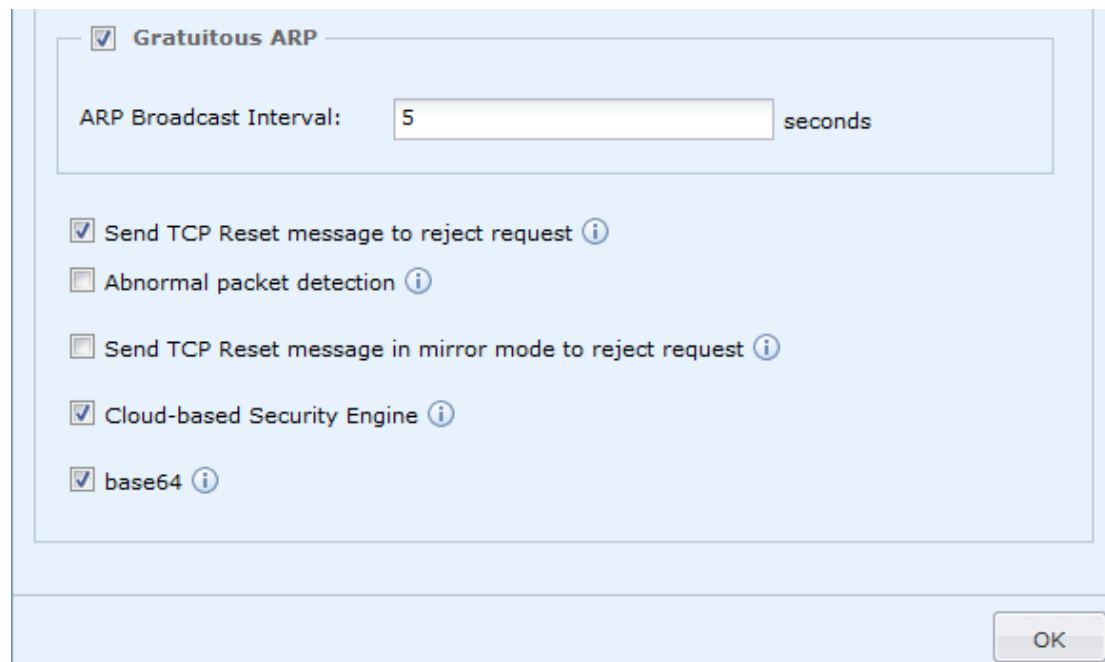
TFTP Port: UDP:69

PPTP Port: TCP:1723

H.323 Port

RAS: UDP:1719

H.225: TCP:1720



☒ **Gratuitous ARP**

ARP Broadcast Interval: 5 seconds

☒ Send TCP Reset message to reject request ⓘ

☐ Abnormal packet detection ⓘ

☐ Send TCP Reset message in mirror mode to reject request ⓘ

☒ Cloud-based Security Engine ⓘ

☒ base64 ⓘ

OK

The parameters **TCP Conn Timeout**, **UDP Conn Timeout**, **ICMP Timeout** define the timeout period of the TCP, UDP, and ICMP connections. If no new data packets are sent over the connection within the period, the connection times out and is dismissed.

The parameters **SSH Port**, **FTP Port**, **RTSP Port**, **SIP Port**, **SQLNET Port**, **TFTP Port**, **PPTP Port**, **H.323 Port**

defines the ports complying different protocols. If the NGAF functions as proxy on the application layer for these protocols and the ports are not default ones, the port information must be modified accordingly.

Free ARP defines whether to enable free ARP broadcasting and the time intervals for sending free ARP broadcasting messages. You are recommended to enable **Free ARP**.

The option **Send TCP Reset message to reject request** enables the NGAF to send a Reset message to disconnect connections after the NGAF turns down a data connection based on configured policies.

The option **Abnormal packet detection** enables the NGAF to discard abnormal TCP packets. Do not enable this function for asymmetric routers not requiring TCP status; otherwise, normal TCP packets may be discarded.

The option **Send TCP Reset message in mirror mode to reject request** enables the NGAF to send TCP RST messages.

The option **Cloud-based Security Engine** allows the NGAF to report suspicious data packets to the cloud-based security engine.

The option **base64** enables the Web application protection mechanism to apply security check on base64 data packets.

Console Configuration

On the **Web UI** tab page for console configuration, you can set the Web UI options and login security options.

In the **Web UI** area, you can set the device name, default code, Web UI port, and timeout period for the NGAF. See the following figure:

The screenshot displays the 'Web UI' configuration window. At the top, there are tabs for 'General', 'System Time', 'Network', 'Web UI' (selected), and 'License'. The 'Web UI Options' section includes a dropdown for 'Language' set to 'English', a text field for 'Device Name' containing 'SANGFOR NGAF', a text field for 'Port' containing '443', and a text field for 'Idle Timeout(min)' containing '10'. Below this is the 'Login Security' section, which contains three text fields: 'Max Concurrent Sessions' (10), 'Per-User Max Logons' (10) with the unit 'locations' to its right, and 'Max Login Attempts' (10). An 'OK' button is located at the bottom right of the window.

Device Name: displayed name of the NGAF.

Default Code: type of code used to identify non-identifiable data monitored by the NGAF. By default, the value is **GBK**.

Port: No. of the port used to set the login console. The default port is TCP 443.

Idle Timeout: timeout period of the console. If the administrator performs no operation within the specified period, the system disconnects by default.

Maximum Concurrent Sessions: maximum number of login users on the NGAF console allowed.

Per-User Max Logons: Maximum number of IP addresses allowed to access the NGAF console using the same administrator account.

Max Login Attempts: Maximum number of login failures allowed for an administrator account.

Click **Submit** to save the configurations and to make the configurations take effect.

License

The licenses of the NGAF includes the gateway license, cross-operator SN, anti-defacement license, function module licenses, and update licenses. See the following figure:

System Time	Network	Web UI	Licensing
Device License			
Gateway ID:		D88CB6EC	
Licensing:		Activated	Modify
Authorization:		Branch VPN Sites: 0 Number of Lines: 2 Mobile VPN Users: 0	
Cross-ISP Access Optimization			
Licensing:		Not activated	Activate
Anti-Defacement License			
Licensing:		Activated	Modify
Authorization:		Websites:	2
License of Function Modules			
Licensing:		Activated	Modify
VPN:		Activated	
Antivirus:		Activated	
IPS:		Activated	
Web Application Protection:		Activated	

Bandwidth Management:	Activated
Application Control:	Activated
Web Filter:	Activated
Data Leak Protection:	Activated
APT Detection:	Activated
Realtime Vulnerability	Activated

Update Licenses		
Anti-Virus Database:	Valid	Modify Expiry Date: 2015-06-19
URL Database:	Valid	Modify Expiry Date: 2015-06-19
Vulnerability Database:	Valid	Modify Expiry Date: 2015-06-19
Software Upgrade:	Valid	Modify Expiry Date: 2015-09-18
Application Ident Database:	Valid	Modify Expiry Date: 2015-06-19
WAF Signature Database:	Valid	Modify Expiry Date: 2015-06-19
Data Leak Protection:	Valid	Modify Expiry Date: 2015-06-19
Malware Signature Database:	Valid	Modify Expiry Date: 2015-06-19

The **License** parameter in the **Device License** area is used to activate the device and authorize license configuration to the NGAF, including the numbers of lines, branch VPN lines, and mobile VPN users

The **License** parameter in the **Cross-ISP Access Optimization** area is used to activate the cross-ISP function of the NGAF.

The **License** parameter in the **Anti-Deface Optimization** area is used to activate the Website anti-defacement function in server protection.

In the **License of Function Modules** area, you can activate different function modules with dedicated licenses, including the VPN, antivirus, IPS, Web application protection, traffic control, application control, Web filter, data leak protection APT Detection and Realtime Vulnerability.

In the **Update Licenses** area, you can activate the updates of policy databases of the NGAF, including the antivirus database, URL database, vulnerability database, software updates, application identification database, Web application protection database, data leak protection database and Malware signature database.

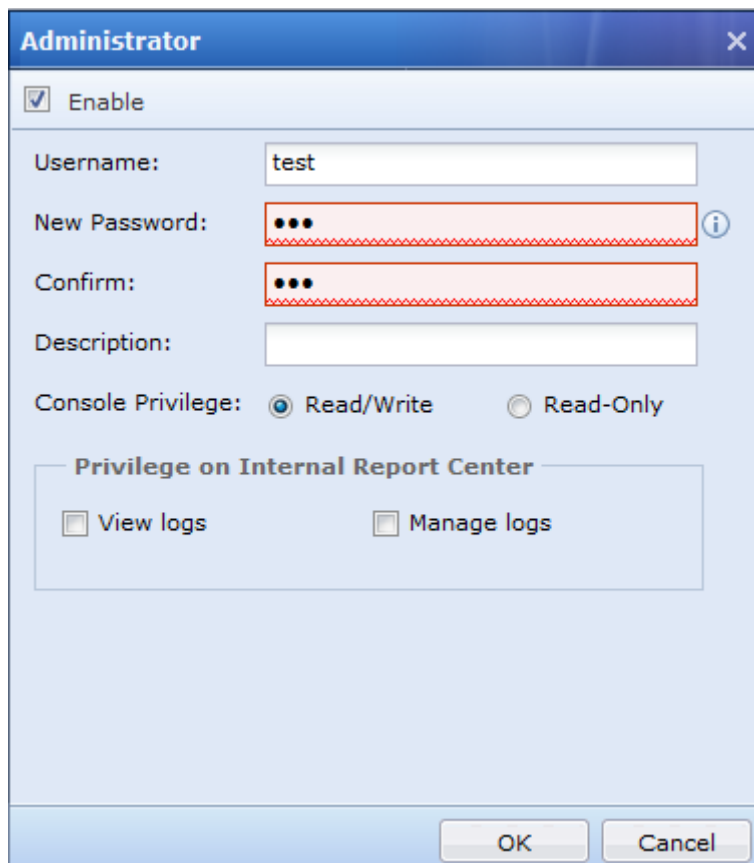
You can click **Modify** and enter the license No. to activate the license.

Administrator Accounts

The administrator accounts are used to manage the users accessing the NGAF console. See the following figure:

Administrator				
+ Add X Delete ✓ Enable ✗ Disable 🔄 Refresh				
<input type="checkbox"/>	No.	Username	Administrative Role	Description
<input type="checkbox"/>	1	admin	administrator	Administrator
				Status
				Delete

Click **Add** to add an administrator account. See the following figure:



The image shows a dialog box titled "Administrator" with a close button (X) in the top right corner. It contains the following fields and options:

- ☒ **Enable**
- Username:** test
- New Password:** [Redacted with three dots]
- Confirm:** [Redacted with three dots]
- Description:** [Empty text box]
- Console Privilege:** ☒ Read/Write ☐ Read-Only
- Privilege on Internal Report Center:**
 - ☐ View logs
 - ☐ Manage logs
- Buttons:** OK, Cancel

User Name: name of the administrator account.

New Password and **Confirm:** password of the administrator account.

Description: description about the account.

Console Privilege - Read/Write: NGAF configuration query and edit rights assigned to the administrator.

Console Privilege - Read-Only: NGAF configuration query rights assigned to the administrator.

View logs: option of assigning database log query rights to the administrator.

Manage logs: option of assigning database log query and delete rights to the administrator. If **Manage logs** is selected, **View logs** is selected by default.

Click **Submit**. The administrator is added.

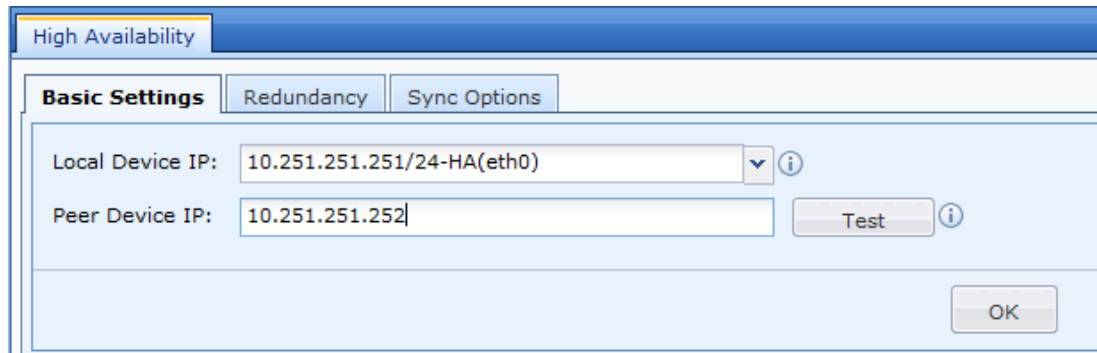
Administrator					
+ Add X Delete ✓ Enable ✗ Disable ↻ Refresh					
<input type="checkbox"/>	No.	Username	Administrative Role	Description	Status
<input type="checkbox"/>	1	admin	administrator	Administrator	✓
<input type="checkbox"/>	2	test	administrator		✓

To manage the existing administrators, click the user name to go to the editing screen. You can click **Delete** to delete the selected administrator account, click **Enable** to enable the selected administrator account, and click **Disable** to disable the selected administrator account.

High Availability

High availability (HA) functions in dual-firewall mode or when two NGAFs work concurrently. Enter **Basic**

Settings > High Availability, as shown in the following figure.



The screenshot shows a configuration window titled "High Availability". It has three tabs: "Basic Settings" (selected), "Redundancy", and "Sync Options". Under the "Basic Settings" tab, there are two input fields: "Local Device IP:" with the value "10.251.251.251/24-HA(eth0)" and a dropdown arrow, and "Peer Device IP:" with the value "10.251.251.252". To the right of the "Peer Device IP" field is a "Test" button. At the bottom right of the window is an "OK" button. Information icons (i) are present next to both IP input fields.

Basic Settings: Sets the local device IP address and peer device IP address. The local device IP address can only be set to the IP address of an interface with HA identification. In addition, this interface transmits and receives heartbeat package information and interactive configuration information, and can communicate with only the interfaces on NGAFs for load balance.

Redundancy: Select **Redundancy** and click Add. The following dialog box is displayed.

Add VRRP Group

VRID: (1-255)

Priority: (1-255)

Preemption: ☐ Yes ☒ No

Heartbeat Interval: (1-60)s

Member Interfaces: ⓘ

<input type="checkbox"/>	No.	Interface	Edit
No data available			

Tracked Interfaces ⓘ

Available:

- eth1
- veth.1

Add ▶

◀ Delete

Selected:

OK Cancel

VRRP Group: Defines the group to which the interface belongs in VRRP mode. Interfaces on two NGAFs or different interfaces on one NGAF can be defined as a VRRP group. The same VRRP group of two NGAFs works in active/standby mode.

Priority: Sets the priority of the selected interface in the Ethernet interface list. The priority increases with the value. The **Priority** setting is effective only after **Preemption** is clicked. If two NGAFs work in redundancy, that is, one NGAF work while the other acts as the standby NGAF and does not work, set **Priority** to **90** and **Preemption** enabled for one NGAF and **Priority** to **80** for the other NGAF. If the NGAF (**Priority** set to **90**) fails, the NGAF (**Priority** set to **80**) takes over the work. After the NGAF (**Priority** set to **90**) is normal, it preempts and works as the active one, while the other becomes standby again.

Preemption: Defines whether active and standby NGAFs preempts to be active. This option must be used with **Priority**.

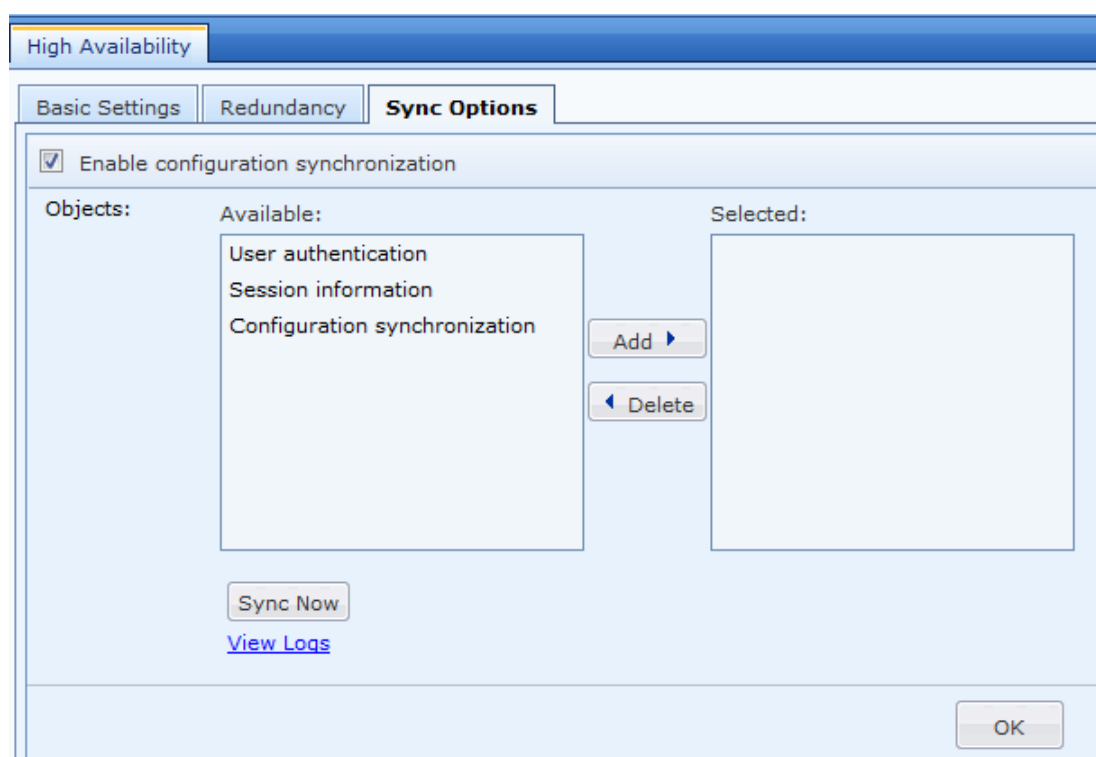
Heartbeat Interval: Sets the interval of data exchanges between two NGAFs. During this interval, the two NGAFs send packages, and notify the Ethernet interface status and link status of each other. If one NGAF is faulty, active/standby switchover is triggered. If both NGAFs fail to receive heartbeat packages, both NGAFs set them as

active and they start to work at the same time.

Member Interfaces: Selects the Ethernet interfaces to be added to the VRRP group. Ethernet interfaces with HA identification cannot be selected here.

Tracked Interfaces: This setting depends on the interface check method defined in interface/area setting. The interfaces will be tracked if selected here. If link monitor is not selected, only Ethernet interfaces in the Ethernet interface list are checked in active/standby mode. Active/standby switchover can be triggered only after physical Ethernet ports are down.

Sync Options: Ignores active/standby attributes of the NGAFs. The modified configuration on one NGAF will be synchronized to the other once the configuration is modified. Select **Enable configuration synchronization**, as shown in the following figure.



Objects: Sets objects to be synchronized between two NGAFs, including **User authentication**, **Session information**, and **Configuration synchronization**. NGAFs check whether configuration changes every 10 seconds.

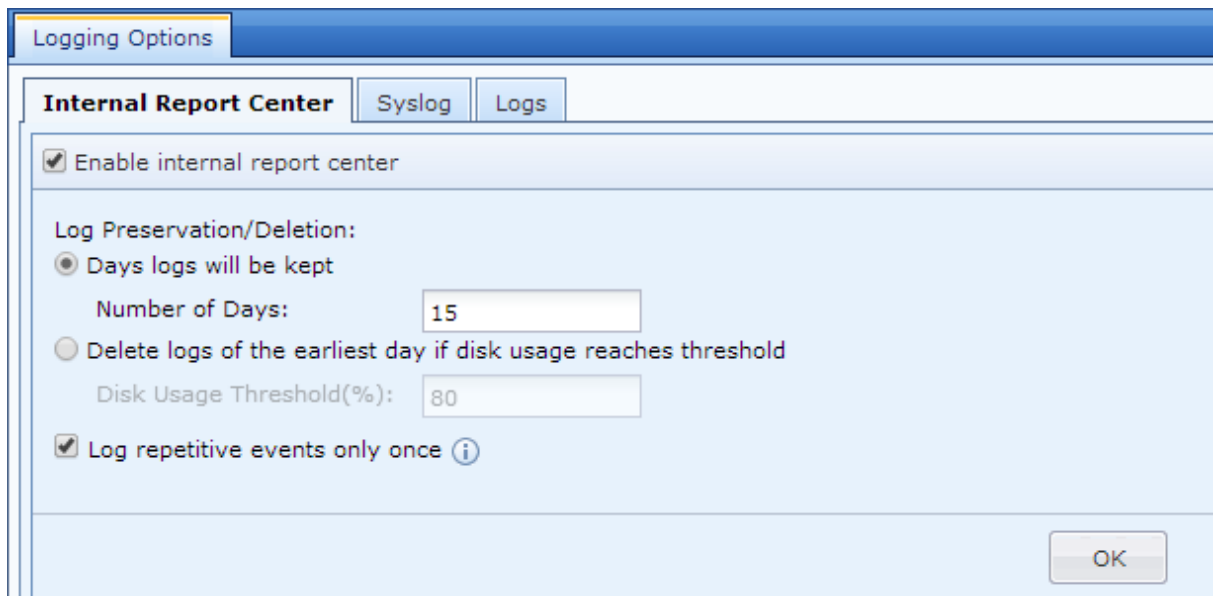


- **Heartbeat Interval for active and standby NGAFs must be the same. Otherwise, active/standby election may experience exceptions.**
- **If the priority of the VRRP group is set to the same value, no preemption occurs no matter ... the Preemption option is clicked.**

- In routing mode, if you enable the link monitor, the active/standby switchover is triggered if any of the three conditions is met: no heartbeat packet received, physical port in DOWN state, link failure after link detection.
- In transparent mode, other ports in the Ethernet interface list will be down once a port is down. The setting does not conflict with interface linkage of interface/area setting. Both settings are valid. That is, if the Ethernet interface list is selected, interface linkage setting is not required.
- Configuration synchronization consists of batch synchronization and incremental synchronization. After a NGAF starts, it sends a configuration synchronization request to the peer and requires synchronization from the peer. In this manner, batch synchronization is performed. After batch synchronization is complete, the NGAF checks whether configuration changes every 10 seconds. Once configuration changes, it synchronizes configuration changes to the peer. In this manner, incremental synchronization is performed.
- If the rule library SN of NGAF A has not expired but that of NGAF B has expired, NGAF A will fail to synchronize the rule library to peer NGAF B after NGAF A upgrades the rule library. Synchronization of other configuration will not be affected.
- Hardware models of two NGAFs in redundancy must be the same. If two NGAFs work in redundancy, Ethernet interfaces will be synchronized. NGAFs in different models have different numbers of Ethernet interfaces, which will result in malfunction of the NGAFs.
- IP address information and High Availability configuration of HA interfaces are not synchronized during configuration synchronization.
- To prevent synchronization from the standby NGAF to the active NGAF and configuration loss on the active NGAF, you are advised to modify configuration only on the active NGAF and enable configuration synchronization of User authentication, Session information and Configuration synchronization on the active NGAF, and to enable configuration synchronization of only User authentication and Session information on the standby NGAF..

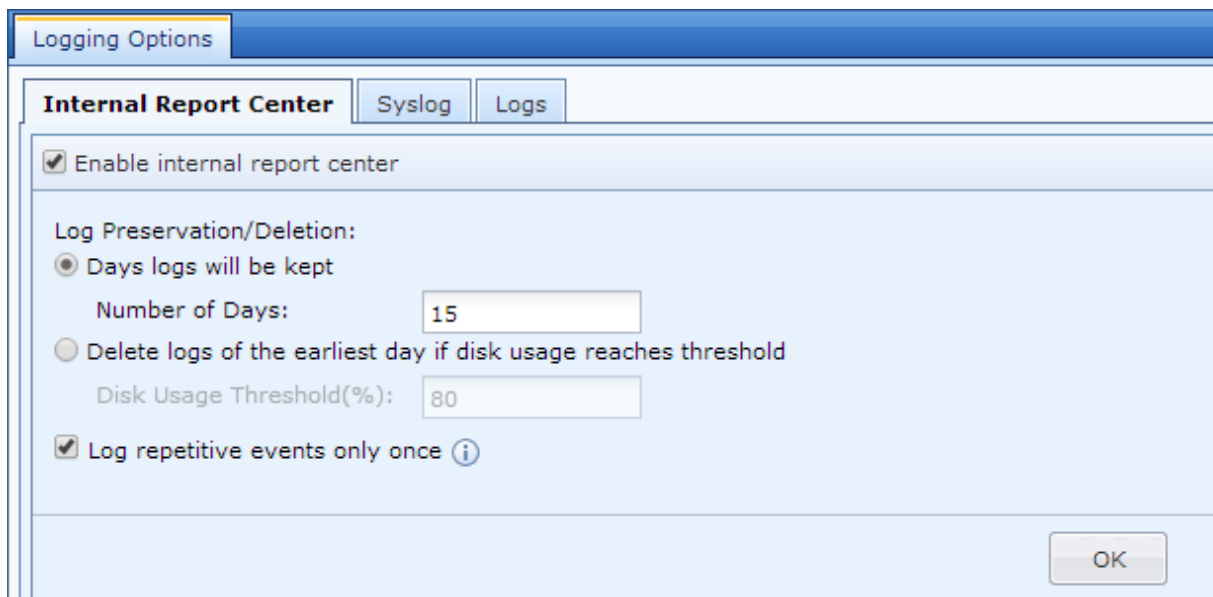
Logging Options

Logging Options sets NGAF log options, including **Internal Report Center** and **Syslog**. **Internal Report Center** includes system logs and data center logs. Syslog can only transmit data center logs but cannot transmit system logs.



Internal Report Center

Internal Report Center: Sets automatic deletion of logs, as shown in the following figure.



Select **Enable internal report center** to enable internal report center of the NGAF.

Log Preservation/Deletion: Sets whether the system automatically deletes access control logs. Click **Days logs will be kept** to set the days of saving logs. Click **Delete logs of the earliest day if disk usage reaches threshold** to set logging according to disk usage.

Log repetitive events only once: After it is selected, the internal report center only logs once for repetitive access to the same domain name, saving disk space.



If Enable internal report center is not selected, the internal report center does not record logs, but it will send the logs to the Syslog server if the Syslog server has been configured.

Syslog Settings

Syslog settings allow NGAF logs saving synchronously to the remote Syslog server. IP address and port of the Syslog server should be set, as shown in the following figure.

The screenshot shows the 'Logging Options' window with the 'Syslog' tab selected. The 'Enable Syslog' checkbox is checked. The 'IP Address' field is set to '10.10.10.10' and the 'Port' field is set to '514'. An 'OK' button is located at the bottom right.



- Syslog supports only UDP connection.
- Syslog can synchronize data report center logs but cannot synchronize system logs.

SMTP Server

SMTP Server sets SMTP server information for the NGAF to send alarm emails.

The screenshot shows the 'SMTP Server' configuration window. The 'Sender Address' field is set to 'test@sangfor.com'. The 'SMTP Server' field is empty. There is a checkbox for 'Require authentication' which is unchecked. Below it are 'Username' and 'Password' fields, both empty. A 'Send Test Email' button is located below the password field. An 'OK' button is at the bottom right.

Sender Address: Sets the mailbox used by the NGAF to send alarm emails, for example, test@domain.com.

SMTP Server: Sets the SMTP server domain name or IP address. If the SMTP server requires user name and password authentication, select **Require authentication**.

Email Send Test Address: Click Send Test Email after the address is entered to check whether the email can be sent.



Site tamper protection has been set in section 3.10.2. If site tampering occurs, email will be sent to the administrator using the SMTP server.

Email alarm set in section 3.13.6 will use the SMTP server.

Email Alarm

Email Alarm enables alarm information to be sent to the administrator's mailbox via email. For example, if the intranet is infected with viruses or the disk usage reaches a threshold, the NGAF automatically sends alarm emails to the administrator's mailbox for alarming.

The screenshot shows the 'Email Alarm' configuration window. At the top, the 'Email Alarm' tab is active. Below it, the 'Enable Email Alarm' checkbox is checked. The main area is divided into two panes. The left pane, titled 'Email Alarm', has a tree view with 'Events' selected. The right pane, titled 'Events', shows a list of 'Alarm-Triggering Events'. The following events are checked with checkboxes: 'Admin login failure', 'Security issue' (which has sub-options 'Anti-virus', 'IPS', 'High', 'Medium', and 'Low' all checked), 'WAF', and 'Internal report center disk usage exceeds threshold'. Below the last event, there is a 'Threshold(%)' field with the value '80' entered. An 'OK' button is located at the bottom right of the window.

Events: Specifies the events that trigger email alarms. If you select multiple events, alarm emails will be triggered when any of the events occurs.

Email Alarm

☒ Enable Email Alarm

Email Alarm

- Events
- Options**

Options

Email Subject: SANGFOR FW Alarm Email Notice

Sending Interval: ☐ Immediately after alarm is triggered
☒ Interval (mins) 20

Recipient Address: support@sangfor.com

OK

Options: Sets information including **Email Subject** and **Sending Interval**.

Globally Excluded Address

Globally Excluded Address sets the IP addresses that are free from monitor and control. Such IP address can be intranet user IP addresses or the IP addresses of the visited destination servers. Domain name exclusion is supported.

Globally Excluded Address

Predefined Excluded Address Custom Excluded Address

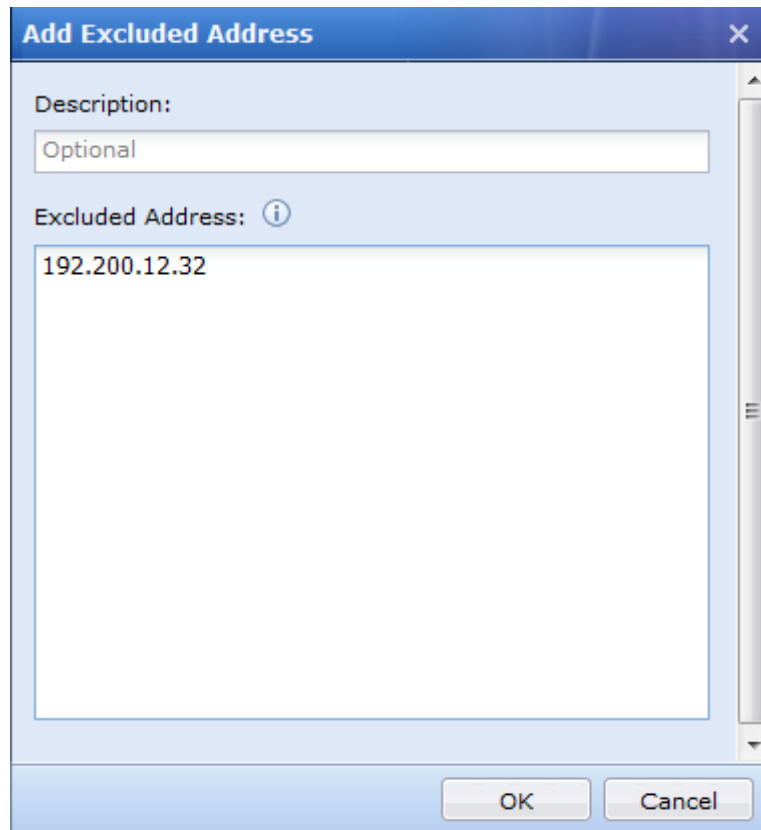
☒ Enable ☐ Disable Search:

<input type="checkbox"/> Excluded Address	Description	Status
<input type="checkbox"/> 360.cn	360.cn	✓
<input type="checkbox"/> rising.com.cn	rising.com.cn	✓
<input type="checkbox"/> 360safe.com	360safe.com	✓
<input type="checkbox"/> update.microsoft.com	update.microsoft.com	✓
<input type="checkbox"/> download.windowsupdate.com	download.windowsupdate.com	✓
<input type="checkbox"/> windowsupdate.microsoft.com	windowsupdate.microsoft.com	✓
<input type="checkbox"/> pccchk.trendmicro.com	pccchk.trendmicro.com	✓
<input type="checkbox"/> activeupdate.trendmicro.com	activeupdate.trendmicro.com	✓
<input type="checkbox"/> kaspersky-labs.com	kaspersky-labs.com	✓
<input type="checkbox"/> jiangmin.com	jiangmin.com	✓
<input type="checkbox"/> liveupdate.symantecliveupdate.c...	liveupdate.symantecliveupdate.c...	✓
<input type="checkbox"/> db.kingsoft.com	db.kingsoft.com	✓
<input type="checkbox"/>	✓

OK

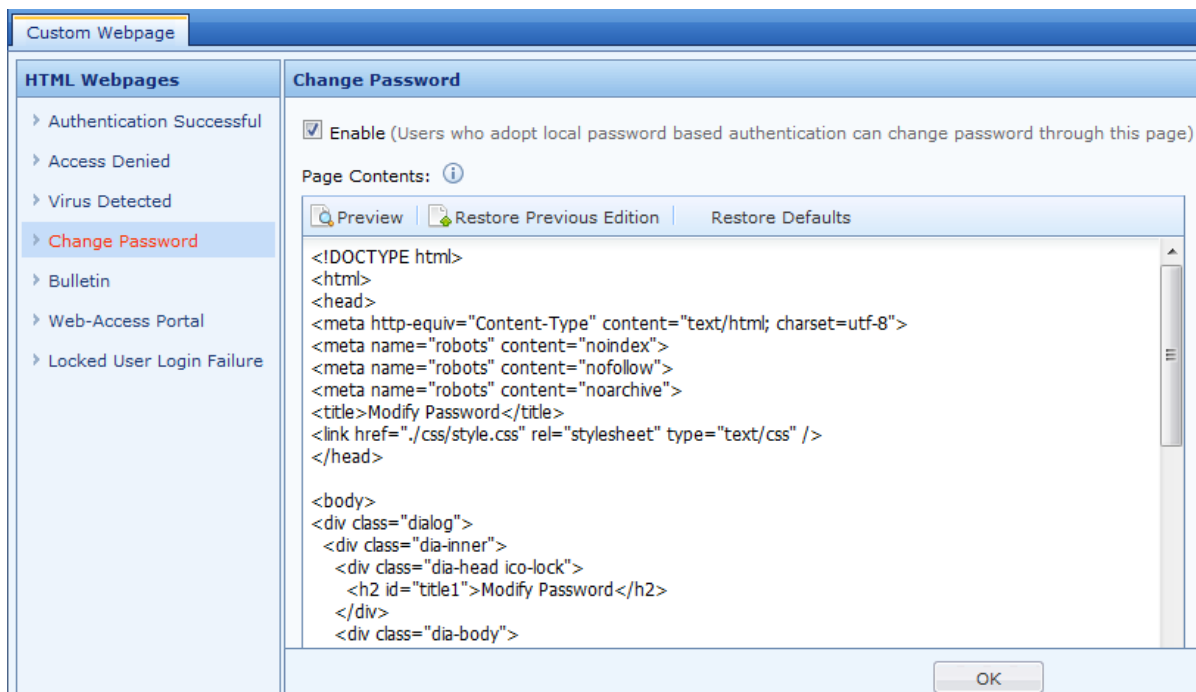
Predefined Excluded Address: Specifies predefined excluded addresses to prevent failure of antivirus software and firewall updates, including IP addresses of these servers. Predefined excluded addresses can be disabled but cannot be deleted.

Custom Excluded Address: Sets the excluded addresses. Click **Add**. On the displayed **Add Excluded Address** dialog box, enter description and the IP addresses to be excluded, and click **OK**.



Custom Webpage

Custom Webpage customizes the webpage redirected to the terminal by the NGAF. The webpages can be customized including **Authentication Successful**, **Access Denied**, **Virus Detected**, **Change Password**, **Bulletin**, **Web-Access Portal**, and **Locked User Login Failure**.



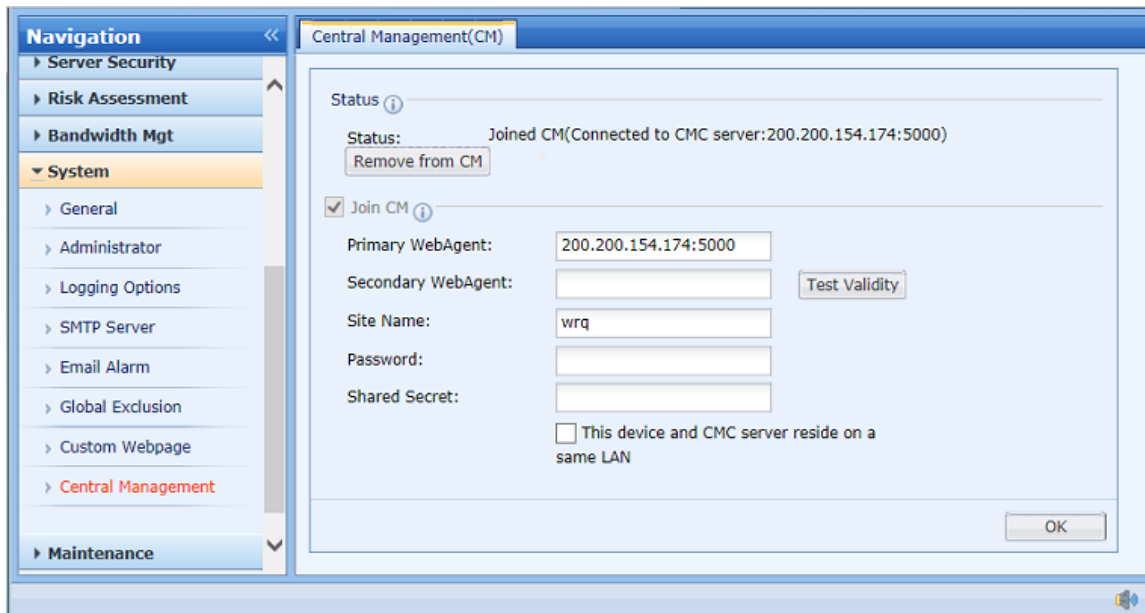
Enable: Select **Enable**, otherwise, the webpage cannot be displayed. Note: **Authentication Successful** and **Web-Access Portal** pages cannot be disabled.

Edit: Modifies the displayed webpages by changing webpage source codes. You are advised to change only the texts and images. Other modifications may lead to missing of normal links.

Click Preview, Save, Restore Defaults, or Restore Previous Edition to preview, save or restore the customized webpages.

Central Management

Sangfor NGAF devices that can be centrally managed and monitored by the Sangfor Central Management Console (CMC) after they connect to the CMC. To have a NGAF device successfully connect to the CMC, create the site on the CMC and configure the CMC connection options on the NGAF device. The Central Management page is shown as below :



Primary WebAgent : Enter the WebAgent address in format of IP:Port or URL. The WebAgent will be used by the site to obtain the network location of the CMC, and therefore it should be the physical IP address or domain name (if available) of the CMC. If the CMC is assigned a WebAgent address by the manufacturer, enter the corresponding URL address.

Test WebAgent : Click it to test the connectivity between the site and CMC. Please note that this button does not work when the WebAgent address is a URL address.

Secondary WebAgent : Secondary WebAgent indicates the standby WebAgent address which will be used by the site to connect to the CMC when the primary WebAgent is unavailable.

Site Name : Enter the username for connecting to the CMC. It should be the name of the corresponding site created on the CMC.

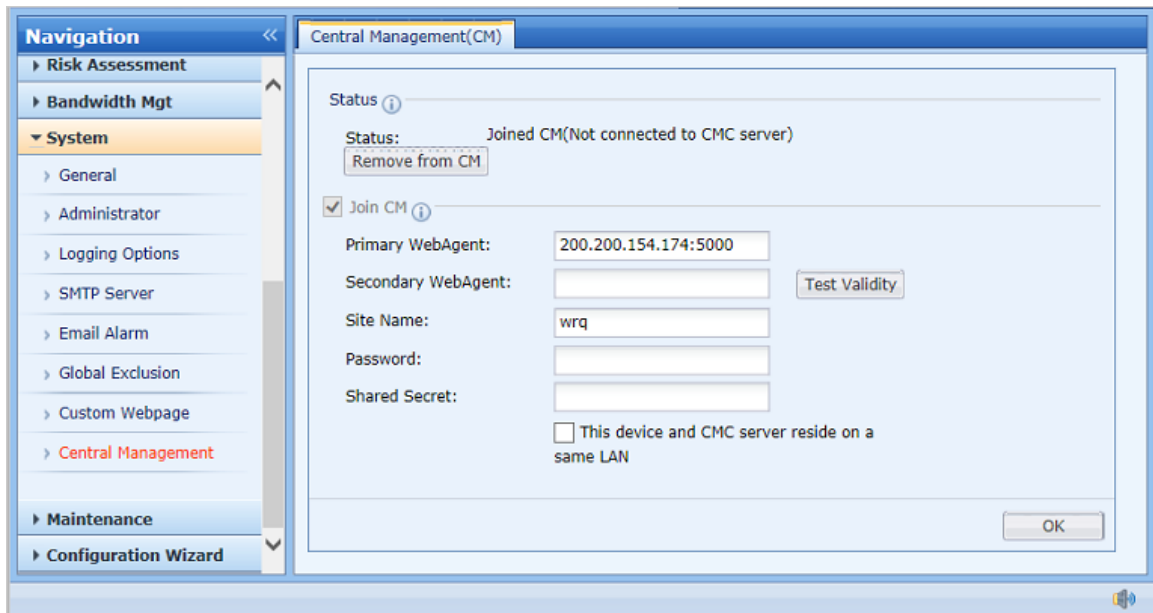
Password : Enter the password for connecting to the CMC. It should be the password of the corresponding site created on the CMC.

Shared Secret : Enter the shared secret which should be the same as that configured on the CMC. Ignore it if no shared secret is set on the CMC.

This device and CMC server reside on a same LAN : Specify whether the CMC resides on the same local area network as the NGAF.

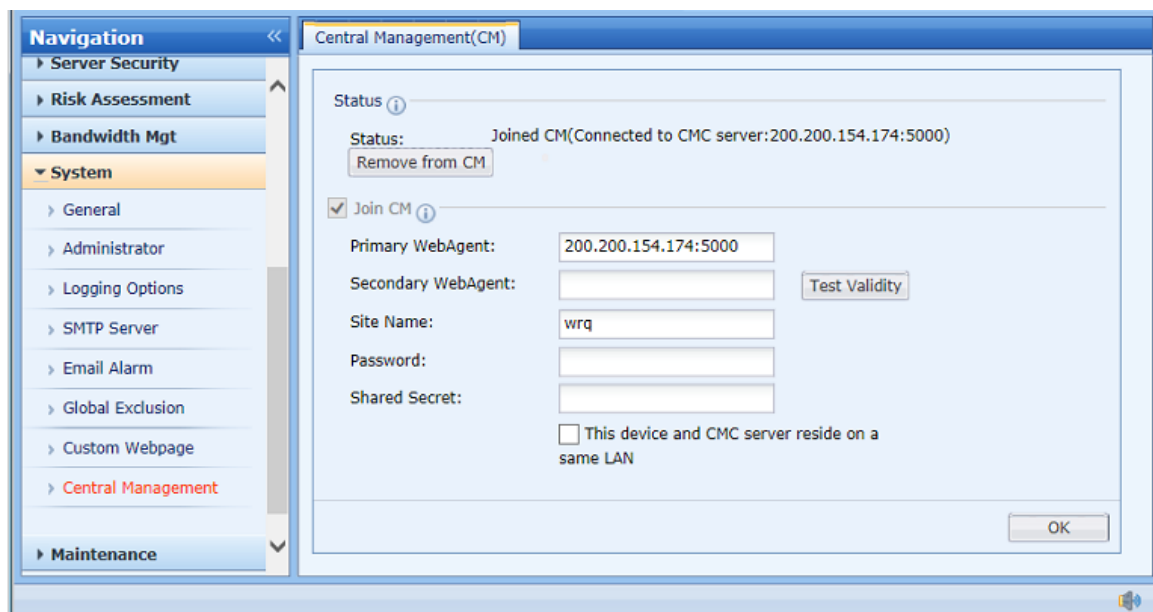
After click **OK**, you should login again.

If the site has joined CM, but it does not connect to the CMC,as shown below:



Please check if the site name, password and shared secret are identical with the site name, password and shared secret configured on the CMC. Otherwise, connecting to the CMC will fail.

If the network connection is available and the site can join Central Management(CM) successfully, you can view the following figure:



System Maintenance

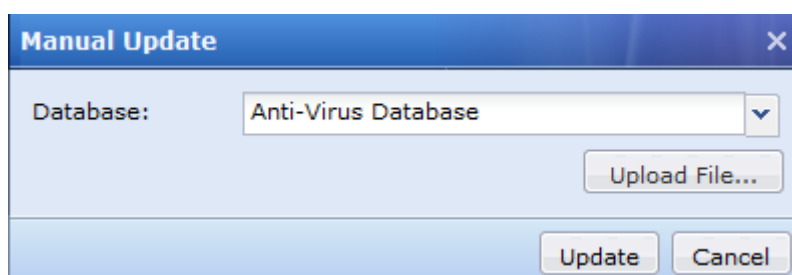
Update

Update manages upgrades of patches and built-in libraries (virus, URL database, IPS signature database, application recognition library, web application protection).

Update							
<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable <input checked="" type="checkbox"/> Manual Update <input checked="" type="checkbox"/> Update Now <input type="checkbox"/> Update Server <input checked="" type="checkbox"/> Refresh Status: Not updating							
<input type="checkbox"/>	No.	Database	Current Version	Latest Version	Update Svc Ex...	Auto Update	Operation
<input type="checkbox"/>	1	Anti-Virus Database	2013-01-04	2013-06-06	2014-07-29	✓	
<input type="checkbox"/>	2	URL Database	2013-04-28	2013-04-28	2014-07-29	✓	
<input type="checkbox"/>	3	IPS	2013-02-16	2013-08-01	2014-07-29	✓	
<input type="checkbox"/>	4	Software Update	--	2013-07-05	Never expire	✓	
<input type="checkbox"/>	5	Application Ident Database	2013-04-02	2013-04-02	2014-07-29	✓	
<input type="checkbox"/>	6	WAF Signature Database	2013-02-16	2013-08-02	2014-07-29	✓	
<input type="checkbox"/>	7	Data Leak Protection	2012-07-04	2012-07-04	2014-07-29	✓	
<input type="checkbox"/>	8	Malware Signature Database	2013-05-13	2013-07-30	2014-07-29	✓	

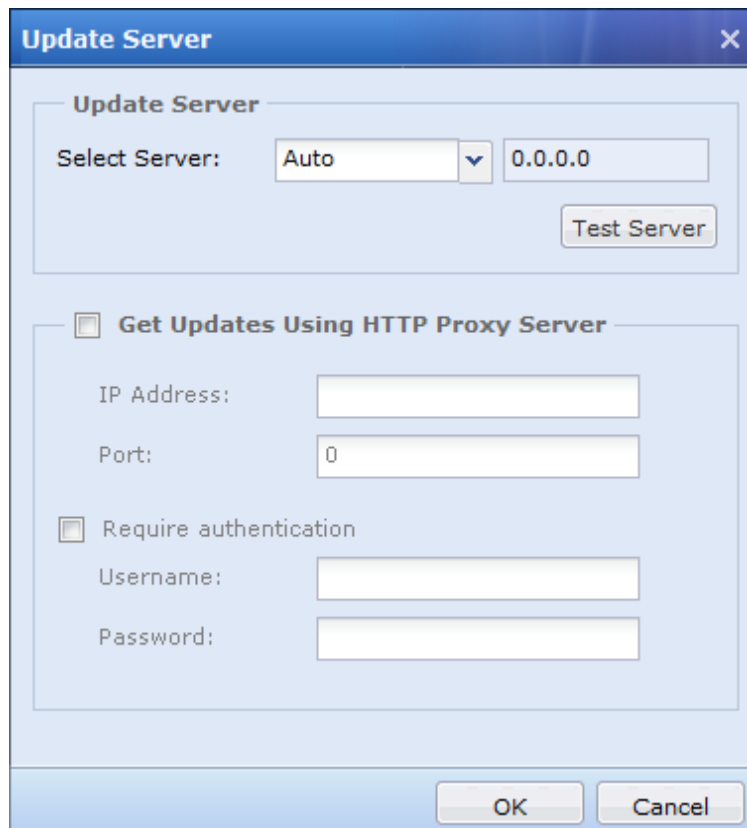
Select the checkbox on the left of **No.** and click Enable to start automatic upgrades of built-in libraries. You can also click Disable to cancel automatic upgrades of built-in libraries and click Refresh to view the real-time information of built-in libraries.

Click **Manual Update** to set manual upgrades of rule libraries within the upgrade validity period, as shown in the following figure.



Click **Update Server** to display the **Update Server** dialog box. **Select Server** sets the server for upgrade. It can be set according to the customer external network link. In addition, you can select **Auto** to enable the NGAF to automatically detect the available update server.

Built-in libraries updates require that the NGAF can access the Internet, or access the Internet through proxy server if any. Select **Get Updates Using HTTP Proxy Server** and set the IP address and port. Then, select **Require authentication** and set the username and password, as shown in the following figure.



Update Server

Update Server

Select Server: Auto 0.0.0.0

Test Server

☐ Get Updates Using HTTP Proxy Server

IP Address:

Port: 0

☐ Require authentication

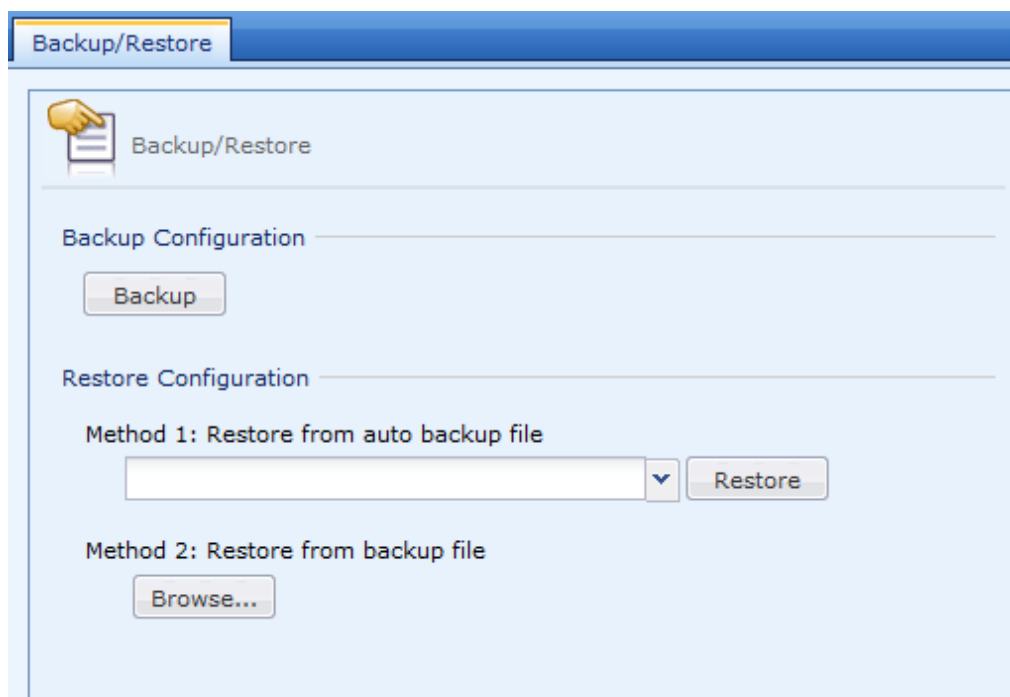
Username:

Password:

OK Cancel

Backup/Restore

Backup/Restore downloads and saves NGAF configuration to the local device, or restores the backup configuration file to the NGAF.



Backup/Restore

Backup/Restore

Backup Configuration

Backup

Restore Configuration

Method 1: Restore from auto backup file

Restore

Method 2: Restore from backup file

Browse...

Backup Configuration: Backs up and download the existing configuration. Click Backup to back up the current configuration.

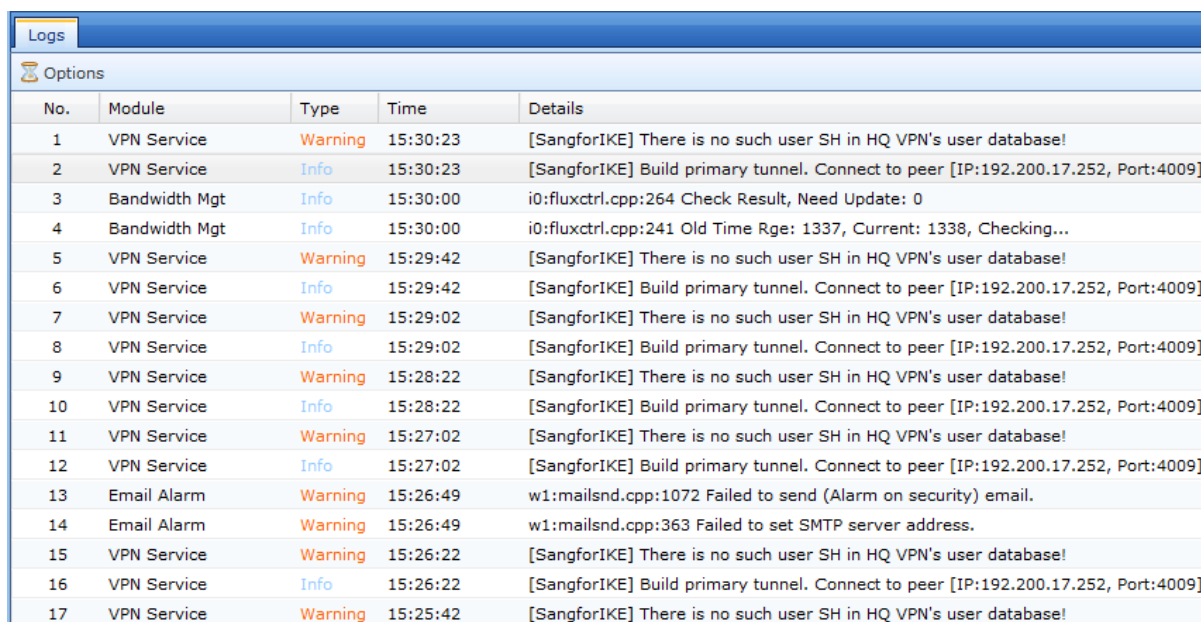
Restore Configuration: Restores backup configuration files in either of the following methods:

Method 1: Restore from auto backup file. The NGAF automatically backs up the configuration every early morning. By default, configuration files in a week are saved. Select the configuration file to be restored and click Restore.

Method 2: Restore from backup file. Click Browse to open a local backup file and click Restore.

Logs

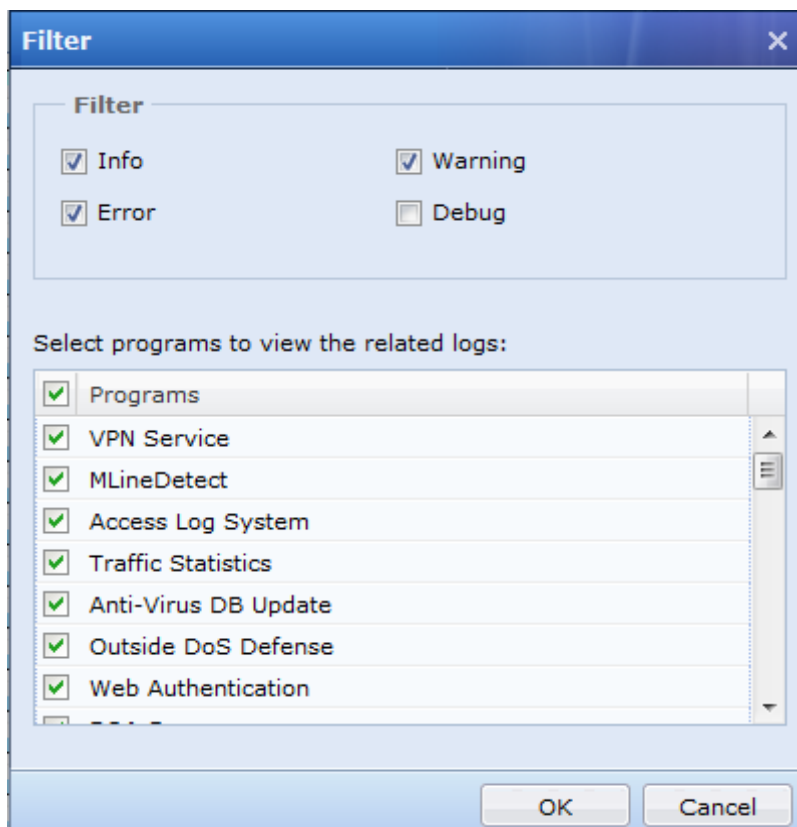
Logs checks operation logs of NGAF modules. You can check whether modules work properly according logs, as shown in the following figure.



The screenshot shows the 'Logs' section of the NGAF interface. It includes a 'Logs' tab and an 'Options' button. Below is a table with columns: No., Module, Type, Time, and Details. The table contains 17 log entries, alternating between 'Warning' and 'Info' types, primarily from the 'VPN Service' and 'Email Alarm' modules.

No.	Module	Type	Time	Details
1	VPN Service	Warning	15:30:23	[SangforIKE] There is no such user SH in HQ VPN's user database!
2	VPN Service	Info	15:30:23	[SangforIKE] Build primary tunnel. Connect to peer [IP:192.200.17.252, Port:4009]!
3	Bandwidth Mgt	Info	15:30:00	i0:fluxctrl.cpp:264 Check Result, Need Update: 0
4	Bandwidth Mgt	Info	15:30:00	i0:fluxctrl.cpp:241 Old Time Rge: 1337, Current: 1338, Checking...
5	VPN Service	Warning	15:29:42	[SangforIKE] There is no such user SH in HQ VPN's user database!
6	VPN Service	Info	15:29:42	[SangforIKE] Build primary tunnel. Connect to peer [IP:192.200.17.252, Port:4009]!
7	VPN Service	Warning	15:29:02	[SangforIKE] There is no such user SH in HQ VPN's user database!
8	VPN Service	Info	15:29:02	[SangforIKE] Build primary tunnel. Connect to peer [IP:192.200.17.252, Port:4009]!
9	VPN Service	Warning	15:28:22	[SangforIKE] There is no such user SH in HQ VPN's user database!
10	VPN Service	Info	15:28:22	[SangforIKE] Build primary tunnel. Connect to peer [IP:192.200.17.252, Port:4009]!
11	VPN Service	Warning	15:27:02	[SangforIKE] There is no such user SH in HQ VPN's user database!
12	VPN Service	Info	15:27:02	[SangforIKE] Build primary tunnel. Connect to peer [IP:192.200.17.252, Port:4009]!
13	Email Alarm	Warning	15:26:49	w1:mailsnd.cpp:1072 Failed to send (Alarm on security) email.
14	Email Alarm	Warning	15:26:49	w1:mailsnd.cpp:363 Failed to set SMTP server address.
15	VPN Service	Warning	15:26:22	[SangforIKE] There is no such user SH in HQ VPN's user database!
16	VPN Service	Info	15:26:22	[SangforIKE] Build primary tunnel. Connect to peer [IP:192.200.17.252, Port:4009]!
17	VPN Service	Warning	15:25:42	[SangforIKE] There is no such user SH in HQ VPN's user database!

Click Options. The Filter dialog box is displayed. Select the log types you want to check, as shown in the following figure.



After OK is clicked, logs of the selected types are displayed.

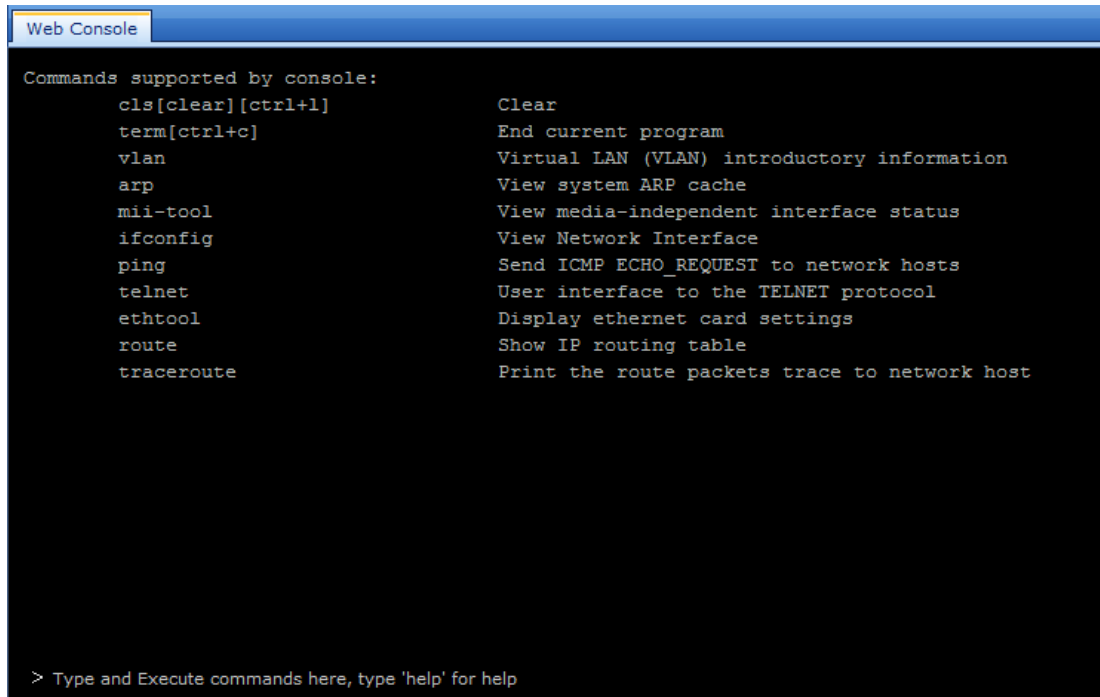
Select a date from the **Date** drop-down list to query system logs on the specified date.



System fault logs of the latest 7 days are saved circularly.

Web Console

Web Console provides simple console commands to query simple information, including **vlan**, **arp**, **mii-tool**, **ifconfig**, **ping**, **telnet**, **ethtool**, **route**, and **traceroute**. The detailed functions of each command are shown in the following figure. Enter a command and press Enter in the Web Console to execute the command.



Packet Drop/Bypass

Packet Drop/Bypass queries which module drops the Packet for what reason. This is used for quick configuration fault location and rule validity verification. Click Enable and Filter. In the displayed **Filter** dialog box, set filter conditions, including **Specified IP**, **IP Whitelist**, **Protocol** and **Port**, as shown in the following figure.

The image shows a 'Filter' dialog box with a blue title bar and a close button (X) in the top right corner. The dialog is divided into three main sections:

- Specified IP**: A section with an information icon (i) and a text input field labeled 'Type here'.
- IP Whitelist**: A section with an information icon (i) and a text input field labeled 'Type here'.
- Protocol**: A section containing:
 - Type:** A dropdown menu currently set to 'All'.
 - Protocol No.:** A text input field with a hint 'Enter an integer between 0 and 255'.
 - Port:** Two radio button options: 'All' (which is selected) and 'Specified Port'. Below 'Specified Port' is a text input field containing the number '0'.

At the bottom of the dialog, there are three buttons: 'Enable Packet Drop List', 'Enable Bypass/Package Drop List', and 'Cancel'.

Specified IP enables the drop list for the specified IP addresses. By default, all network segments are included.

IP Whitelist excludes IP addresses from **Specified IP** so that real-time log drop and bypass are disabled for these IP addresses.

Protocol and **Port** define the protocol type and port of Packets whose drop status is output to the access control list.

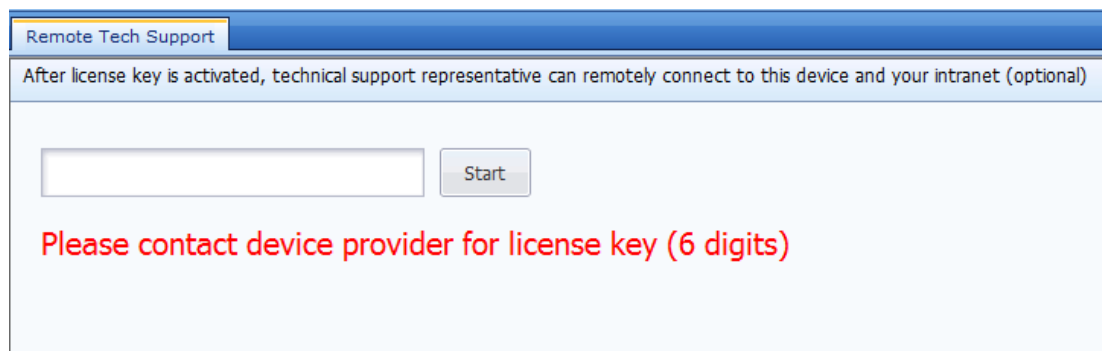
Click **Enable Packet Drop List** to validate the drop list. All policies of the NGAF are valid and packets complying with drop policy configuration will be dropped and displayed. You can click **Refresh** to view the dropped packets in real time.

Click **Enable Bypass/Package Drop List** to validate the drop list and bypass. Network access policies are invalid and packets complying with drop policy configuration will be bypassed and displayed. You can click **Refresh** to view the dropped packets in real time. This function can promptly check whether errors such as network disconnection are caused by the fault in the network access behavior module, and restore network failures caused by policy configuration faults.

Cancel disables the drop list output and bypass.

Remote Tech Support

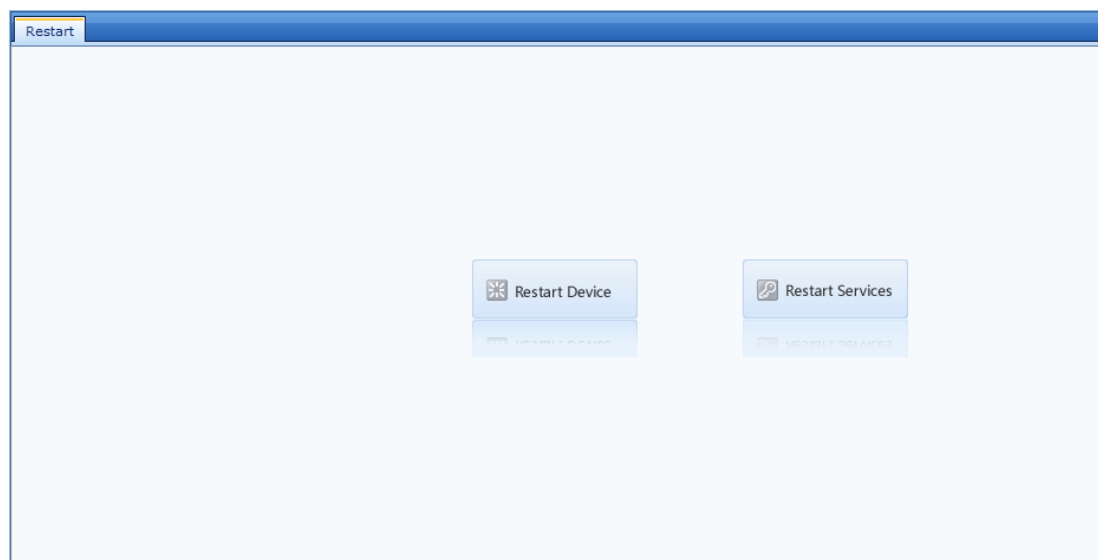
This function is used when device connection fails through port mapping. Enter the license key provided by the device provider and click Start. Then, technical support personnel can connect to your device and intranet.



The interface for Remote Tech Support. It features a blue header bar with the text "Remote Tech Support". Below the header, a light blue box contains the text: "After license key is activated, technical support representative can remotely connect to this device and your intranet (optional)". Below this box is a white input field for a license key and a "Start" button. At the bottom, a red text message reads: "Please contact device provider for license key (6 digits)".

Restart

The **Restart** page provides Restart Device and Restart Services buttons, as shown in the following figure.



Configuration

Device as a Gateway (Routing Mode)

If the NGAF device functioning as a gateway is deployed, configure the device as follows:



This Device as Gateway

This is often used on initial installation to ensure normal network operation

1. [Physical Interface](#)

- a. Set interface type to route
- b. Configure physical interface as WAN interface for connecting to external network.

2. [Zone](#)

- a. Assign the configured interfaces to appropriate zone according to security level.

3. [IP Group](#)

- a. Put local IP addresses into different IP groups that can associate with security policy.

4. [Static Route](#)

- a. Make sure this device can communicate with the internal and external network normally.

5. [NAT](#)

- a. Create SNAT rule to translate source addresses of outgoing packets to public IP address.
- b. Create DNAT rule to translate destination addresses of incoming packets.



Click Physical Interface and a **Physical Interface** configuration window is displayed. You can configure routing interfaces, interface addresses, and interface attributes in this window.

Click Zone and a **Zone** configuration window is displayed. You can assign Ethernet ports to different areas.

Click IP Group and you can enter **Object Definition > IP Group** path.

Click Static Route and you can enter **Network Configuration > Route > Static Route** configuration path.

Click NAT and you can enter **Firewall > NAT** path. If the NGAF device connects to an interface of a public network and uses a proxy for intranet to access internet, the source address needs to be translated. If the intranet server is pushing messages to a public network, the destination address needs to be translated.



After a new NAT is created, you need to create an application control policy under Content Security >

Application Control Policy.

Data Mirroring (Bypass Mode)

If the NGAF device is deployed in a bypass mode to fulfill functions of IPS, WAF, and data leakage prevention, configure the device as follows:



Data Mirroring

This device is connected to a mirroring port, requiring no change to existing network topology.

1. [Physical Interface](#)


- a. Set an interface to mirror port
- b. Set manage interface



Click Physical Interface and a **Physical Interface** configuration window is displayed. You can set the interface type to bypass mirroring interface to mirror data from the switch.

No Change to Existing Network (Bridge Transparent Mode)

If the NGAF device is deployed without any changes to the existing network, that is, the NGAF device is deployed as a transparent bridge in the network, configure the device as follows:



No Change to Existing Network

At the uplink of data center, transparent to and requiring no change to existing network.

- [1. Physical Interface](#)
 - Set interface type to transparent
 - Set the outside interface to WAN interface to distinguish inbound and outbound traffic.
- [2. Zone](#)
 - Assign the configured interfaces to appropriate zone according to security level.
- [3. IP Group](#)
 - Put local IP addresses into different IP groups that can associate with security policy.

Click Physical Interface and a **Physical Interface** configuratoin window is displayed. You can set the interface type to transparent interface with the uplink interface set to WAN, so that you can measure data volume in the uplink and downlink.

Click Zone and a **Zone** configuration window is displayed. You can assign Ethernet ports to different areas.


Click IP Group and you can enter **Object Definition > IP Group** path.



After the device is configured to the transparent mode, you need to create an application control policy under Content Security > Application Control Policy. Otherwise data cannot go through the device.

User Authentication

If an intranet user accesses the internet after being authenticated, configure the device as follows:



User Authentication

Set authentication method for connecting users and associate with authentication policy.

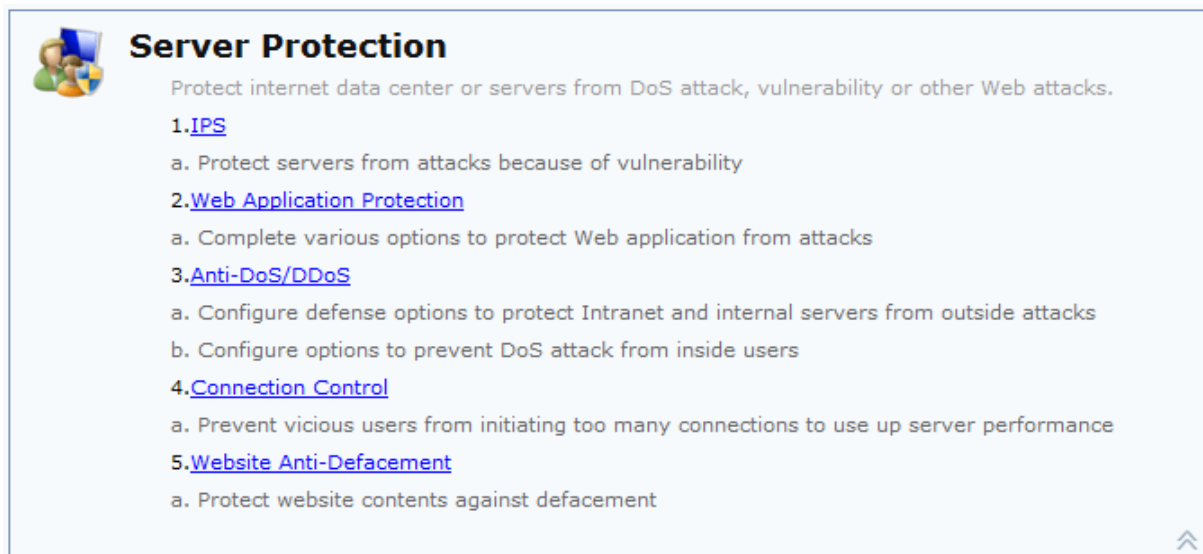
- [1. Local Users](#)
 - Create and import user and group.
- [2. Authentication Policy](#)
 - Enable user authentication and select the zone that needs to be authenticated.
 - Configure authentication policy

Click **Local Users** and you can enter **Authentication System > User Management > Group/User** path to add a user or user group.

Clicke **Authentication Policy** and you can enter **Authentication System > User Management > User Authenticaiton** path to configure authentication zones and modes.

Server Protection

If a server is deployed in the intranet, configure the device as follows:



Click **IPS** and an **IPS** window is displayed. You can add an IPS rule to protect the server.

Click **Web Application Protection** and you can enter the **Server Protection > Web Application Protection** path to enable a protection mode for the server.

Click **Anti-DoS/DDoS** and you can enter **Firewall > Anti-DoS/DDoS** path to configure intranet and server protection against internet risks, or configure an intranet DoS protection to prevent intranet risks.

Click **Connection Control** and you can enter **Firewall > Connection Control** path. You can control the connection of users from certain zones or IP groups to prevent a vicious consumption on server performance.

Click **Website Anti-Defacement** and you can enter **Server Protection > Website Anti-Defacement** path to configure anti-defacement function against websites.

Internet Access Protection

If intranet users have a secured access to the internet, configure the device as follows:



Click **IPS** and an **IPS** window is displayed. You can add an IPS rule to protect the server.

Click **Application Control** and you can enter **Content Security > Application Control Policy** path to add trusted applications being visited by users from intranet zones or IP groups.

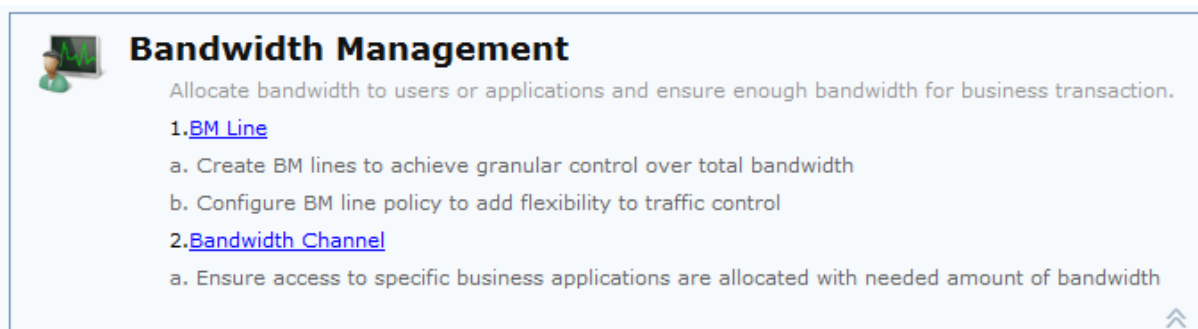
Click **Anti-virus** and you can enter **Content Security > Anti-virus Policy** path. You can configure anti-virus policies on HTTP, FTP, SMTP, and POP3 applications being visited by users from source and destination zones and IP groups.

Click **Web Filter** and you can enter **Content Security > Web Filter** path. You can filter and protect user actions that matches policies configured for the source zones and IP groups, so that you can prevent users from risks brought by add-ins and scripts carried on websites.

Click **Anti-Malware** and you can enter **Content Security > Anti-Malware** path. You can add a risk isolation policy to prevent botnets and Trojans from access the clients.

Bandwidth Management

If you need to guarantee the bandwidth for important applications used by intranet users, configure the device as follows:




Click **BM Line** and you can enter **Traffic Management > BM Line Configuration** path to configure internet bandwidth and BM line rules.

Click **Bandwidth Channel** and you can enter **Traffic Management > Bandwidth Channel** path. You can configure the minimum uplink and downlink bandwidth of certain applications for users or IP groups, so that important

applications have sufficient bandwidth when the traffic is busy.

Set Attack Reminder and Keep Track of Attacker

If a server or client is attacked or matches a certain security policy, configure the device as follows to inform the administrator and record logs:



Set Attack Reminder and Keep Track of Attacker

Alarm will be given and event be logged when attack is detected

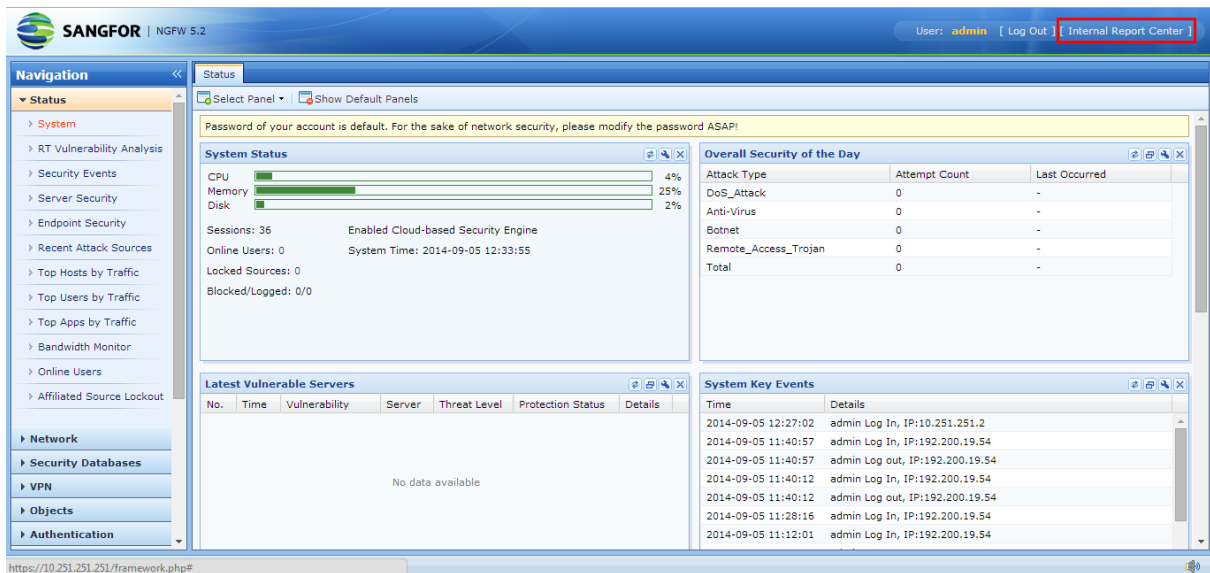
1. [Email Alarm](#)
 - a. Configure the alarm options and email address to receive alarm triggered by attack attempt
2. [Logging Options](#)
 - a. Configure external report center to store firewall logs

Click **Email Alarm** and you can enter **System > Email Alarm** path to configure the mail server which events need to be reported is delivered to.

Click **Logging Options** and you can enter **System > Logging Options** path to configure the logging policy for local logs, or send log files to the Syslog server and being restored.

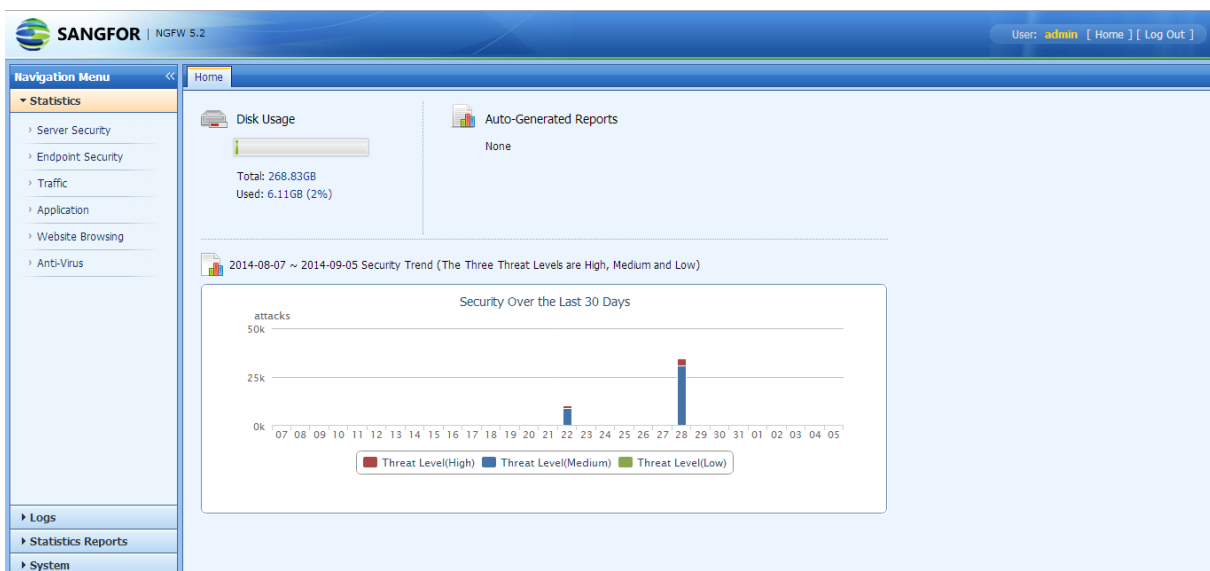
Data Center

The data center enables users to search and collect statistics on the logs generated by function modules. For example, a user can search for the attacks blocked by web application protection and identify the source and destination IP addresses of the attacks, or calculate the DoS attacks on servers over a specified period. To access the data center, click **Internal Report Center** in the upper right corner.



Statistics

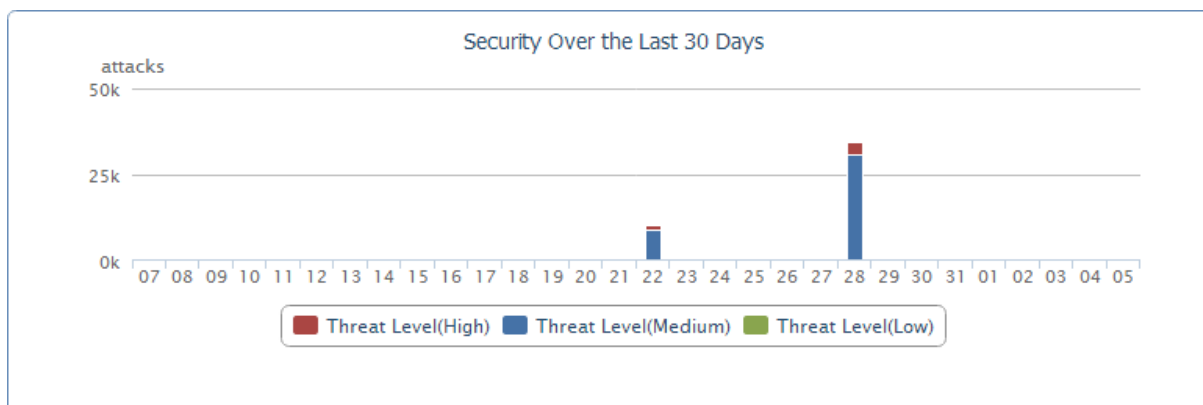
The home page of the data center displays the security trend and traffic rate trend over the last 30 days.



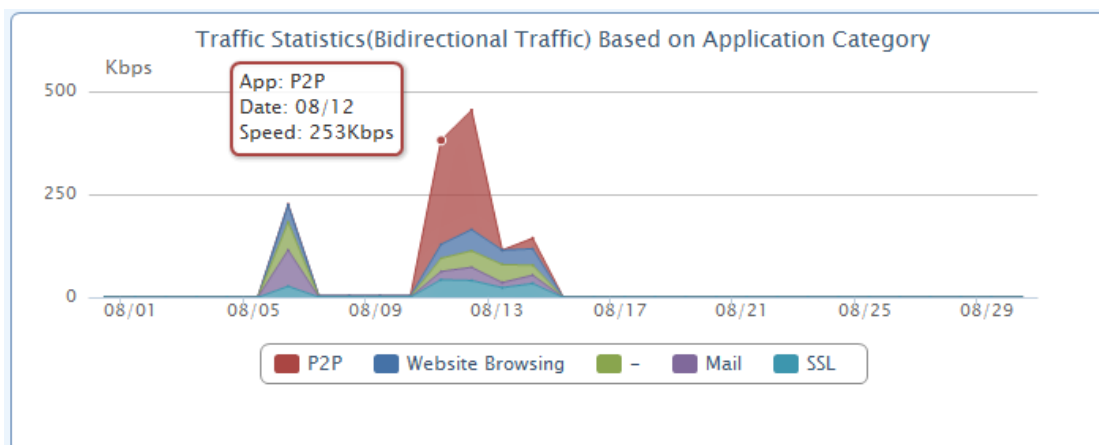
Disk Usage: indicates the used percentage of the current disk. The preceding figure shows that 3% of the disk space is used.

Security Over the Last 30 Days: shows the security trend over the last 30 days. The security described here

includes antivirus, ActiveX filter, script filter, DoS attacks, IPS attacks, and security threats detected by WEB application protection. To view attack details, move the cursor to the corresponding column. The following figure shows that there are 34.5 thousand attacks occurred on day 28. The x axis indicates time and the y axis indicates the number of attacks.



Traffic Statistics: shows the top 5 applications with the largest traffic rate over the last 30 days. The following figure shows that the traffic rate of the P2P application reached 253 KB/s on August 12. The x axis indicates time and the y axis indicates the traffic rate.



Server Security

The **Server Security** page (shown in the following figure) shows the number of server attacks, including DoS attacks from the Internet, IPS attacks, and attacks blocked by the web application protection module.

Navigation Menu

▼ Statistics

> Server Security

> Endpoint Security

> Traffic

> Application

> Website Browsing

> Anti-Virus

> Logs

> Statistics Reports

> System

Server Security

Specify the following and click Go to retrieve data.

Filter

Period: This month 2013-08-01 - 2013-08-31

Server IP: All

Attack Type: All

Threat Level: ☒ High ☒ Medium ☒ Low

Action: ☒ Allow ☒ Deny

Others

Statistics: ☒ Target Server ☐ Attack Type ☐ Attack Source

Show Top: 10

Chart Type: ☒ Ranking ☐ Trend ☐ Ranking & Trend

Less <<

Go

☐ Open in new tab

Example

Application scenario: A user needs to show the number and percentage of web application attacks on all servers on the intranet on May 30. The statistics are displayed based on the top 10 attacked servers.

Step 1: Set statistic criteria.

SANGFOR NGAF 6.4 User Manual

369

Server Security

Specify the following and click Go to retrieve data.

Filter

Period: 2013-08-15 - 2013-08-15

Server IP:

Attack Type:

Threat Level: ☒ High ☒ Medium ☒ Low

Action: ☒ Allow ☒ Deny

Others

Statistics: ☒ Target Server ☐ Attack Type ☐ Attack Source

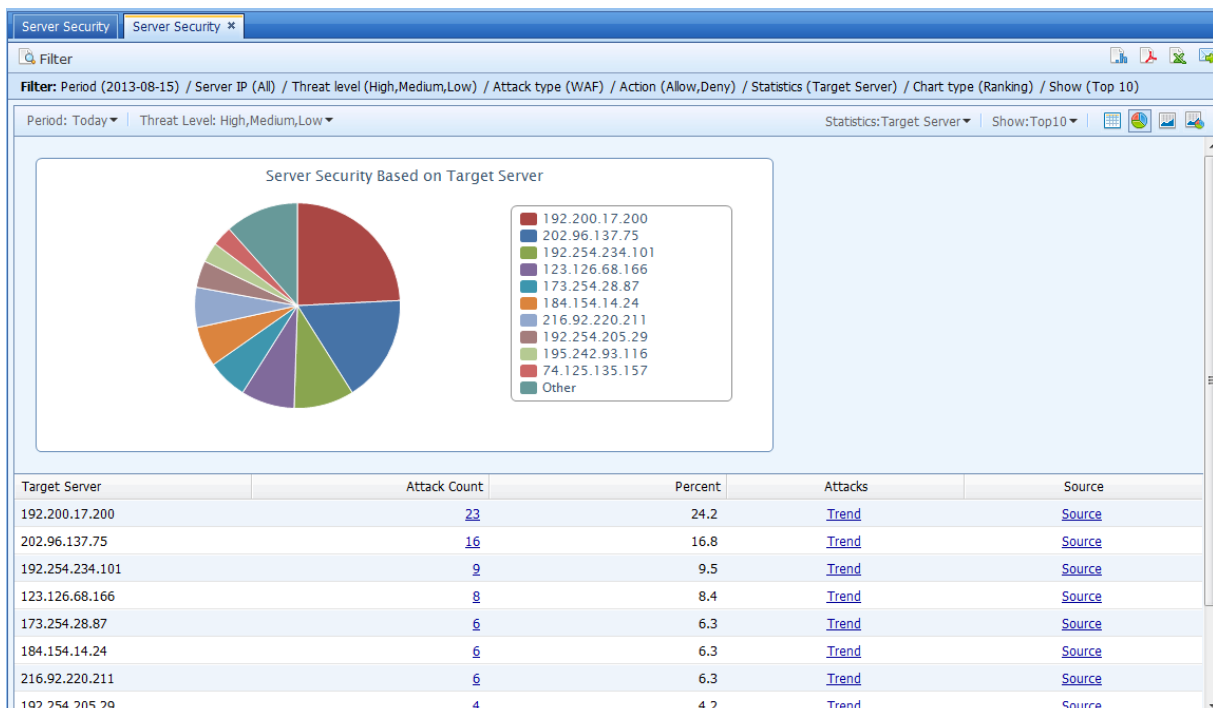
Show Top:

Chart Type: ☒ Ranking ☐ Trend ☐ Ranking & Trend

[Less <<](#)

☒ Open in new tab

Step 2: Click **Go**. A report is generated automatically.



Step 3: To view the type of web application attack on the server with the IP address 10.10.1.1, click the corresponding attack count to link to attack details.

Server Security				
Server Security * Attack Count *				
Filter: Period (2013-08-15) / Server IP (192.200.17.200) / Threat level (High,Medium,Low) / Attack type (WAF) / Action (Allow,Deny) / Statistics (Attack Type) / Chart type (Ranking) / Show (Top 10)				
Show:Top10				
Attack Type	Attack Count	Percent	Attacks	Drill-Down
HTTP error page filter	23	100	Trend	Source

The data shows that all attacks on the server are SQL injection attacks, totaling 3509 times.



To enable the data center to collect statistics on server security logs, click **Log event** in the **Action** area on the console.

Endpoint Security

The **Endpoint Security** page enables users to collect statistics on the number and percentage of DoS attacks, IPS attacks, and virus attacks mounted on the intranet by intranet users.

Endpoint Security

Specify the following and click Go to retrieve data.

Filter

Period: Today 2013-08-15 - 2013-08-15

IP/User: All IP User Group

Attack Type: All

Threat Level: High Medium Low

Action: Allow Deny

Others

Statistics: Host IP Attack Type

Show Top: 10

Less <<

Go Open in new tab

Example

Application scenario: A user needs to show the top 10 IPS attacks on intranet users on August 15.

Step 1: Set statistic criteria.

Endpoint Security

Filter

Specify the following and click Go to retrieve data.

Filter

Period: Today 2013-08-15 - 2013-08-15

IP/User: ☒ All ☐ IP ☐ User ☐ Group

Attack Type: IPS

Threat Level: ☒ High ☒ Medium ☒ Low

Action: ☒ Allow ☒ Deny

Others

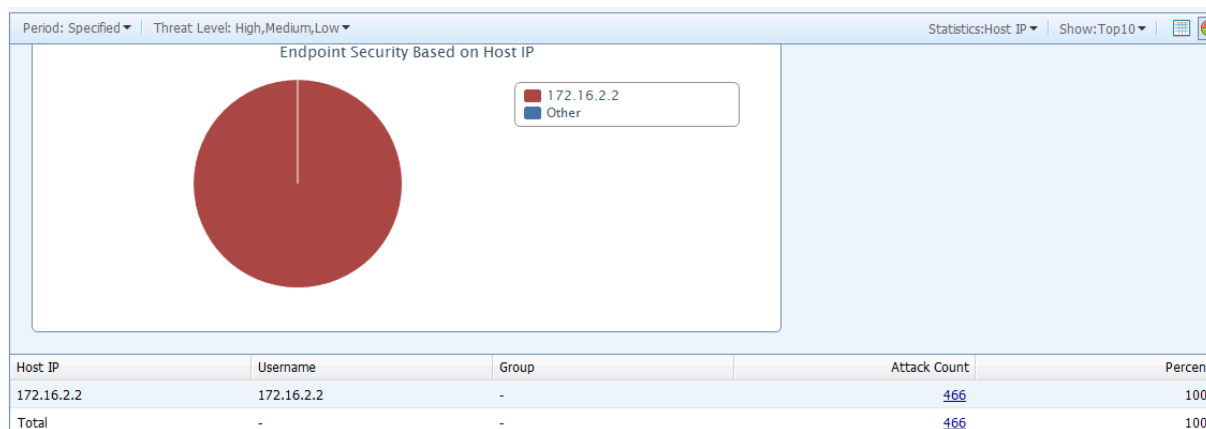
Statistics: ☒ Host IP ☐ Attack Type


Show Top: 10

Less <<

Go Cancel ☒ Open in new tab

Step 2: Click **Go**. Corresponding icons are generated.



To generate a report, generate a PDF file, export data to an EXCEL file, or send data as an email, click the corresponding button in  in the upper right corner.



To enable the data center to collect statistics on server security logs, click Log event in the Action area on the console.

Traffic Statistics

The **Traffic** page enables users to collect statistics on the Internet access traffic of intranet users by application, IP address, etc.

The screenshot shows a web interface titled "Traffic". Below the title bar, there is a light blue box with a document icon and the text "Specify the following and click Go to retrieve data.".

Filter

- Period: A dropdown menu set to "Today" and a date range from "2013-08-15" to "2013-08-15".
- Schedule: A dropdown menu set to "All week".
- IP/User: Radio buttons for "All" (selected), "IP", "User", and "Group".
- Application: A text input field containing "All" and a small icon to the right.

Others

- Statistics: Radio buttons for "App Category" (selected), "Application", "Group", and "IP/User".
- Rank By: Radio buttons for "Bidirectional Traffic" (selected), "Outbound Traffic", and "Inbound Traffic".
- Show Top: A text input field containing "10" with a small icon to the right.
- Chart Type: Radio buttons for "Ranking" (selected), "Trend", and "Ranking & Trend".

At the bottom left, there is a "Less <<" link. At the bottom right, there is a "Go" button and a checkbox labeled "Open in new tab".

Example

Application scenario: A user needs to show the top 10 IP addresses of intranet users occupying the heaviest traffic on August 15.

Step 1: Set statistic criteria.

Traffic

Filter

Specify the following and click Go to retrieve data.

Filter

Period: Today 2013-08-15 - 2013-08-15

Schedule: All week

IP/User: ☒ All ☐ IP ☐ User ☐ Group

Application: All

Others

Statistics: ☒ App Category ☐ Application ☐ Group ☐ IP/User

Rank By: ☒ Bidirectional Traffic ☐ Outbound Traffic ☐ Inbound Traffic

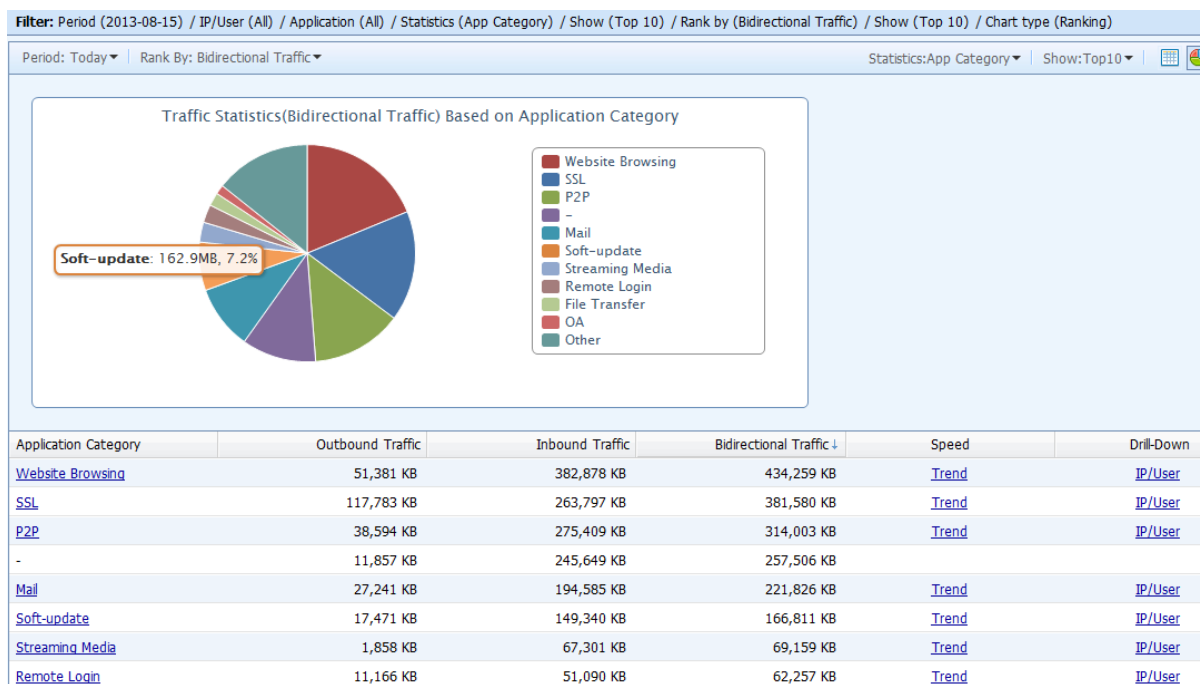
Show Top: 10

Chart Type: ☒ Ranking ☐ Trend ☐ Ranking & Trend

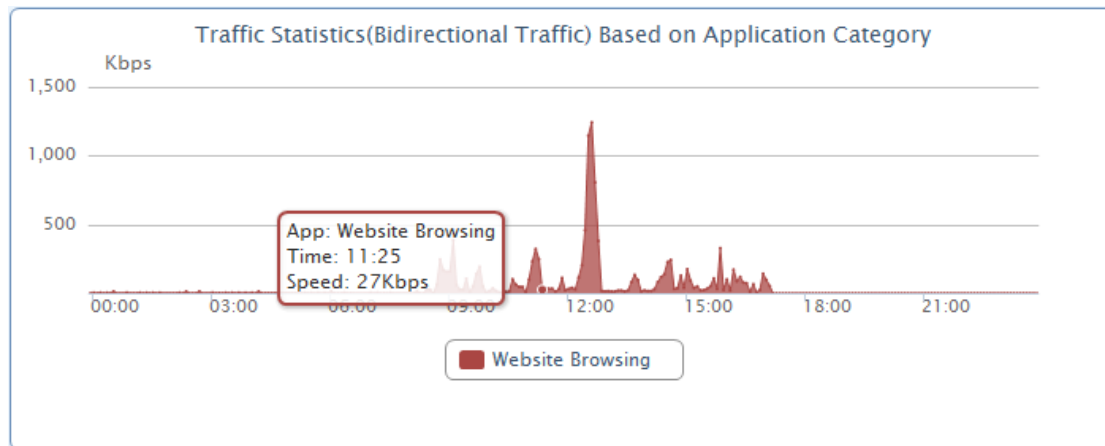
[Less <<](#)

Go Cancel ☒ Open in new tab

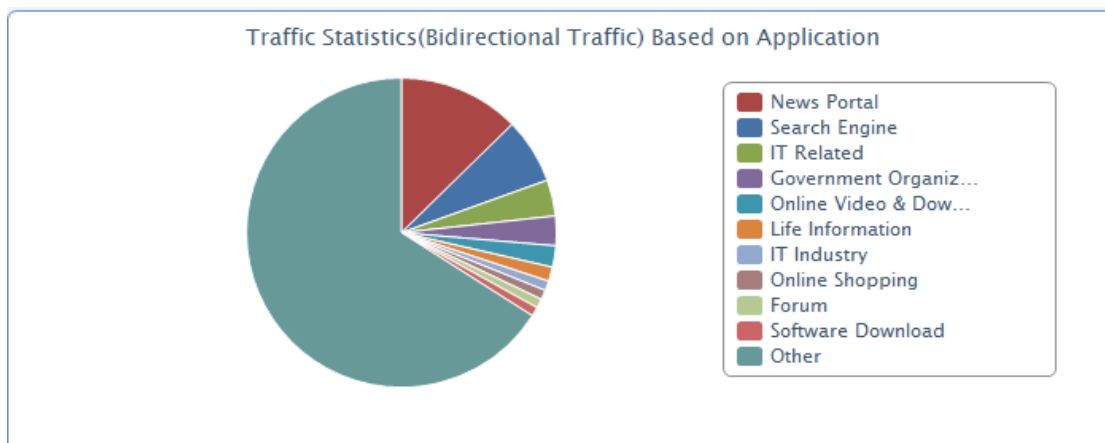
Step 2: Click **Go**. Relevant data is generated.




Click **Trend**. The traffic rate trend of the specified IP address on May 30 is displayed.



Click **Application Category**. The traffic composition of the specified IP address is displayed



To generate a report, generate a PDF file, export data to an EXCEL file, or send data as an email, click the corresponding button in  in the upper right corner.




The traffic statistics function is enabled by default, thus requiring no relevant operation on the console.

Application Statistics

The **Application** page enables users to collect statistics on the times intranet users access an application on the Internet. For example, a user can identify the applications that are accessed by intranet users most frequently.

Application

 Specify the following and click Go to retrieve data.

Filter

Period:
Today
2013-08-15
-
2013-08-15
Schedule:
All week
IP/User:
All
IP
User
Group
Application:
All
Action:
Allow
Deny

Others

Statistics:
App Category
Application
IP/User
Show Top:
10

Less <<


Go
☐ Open in new tab

Example

Application scenario: A user needs to show the top 10 applications that are accessed by intranet users most frequently from August 12 to 15.

Step 1: Set statistic criteria.

Application

 Specify the following and click Go to retrieve data.

Filter

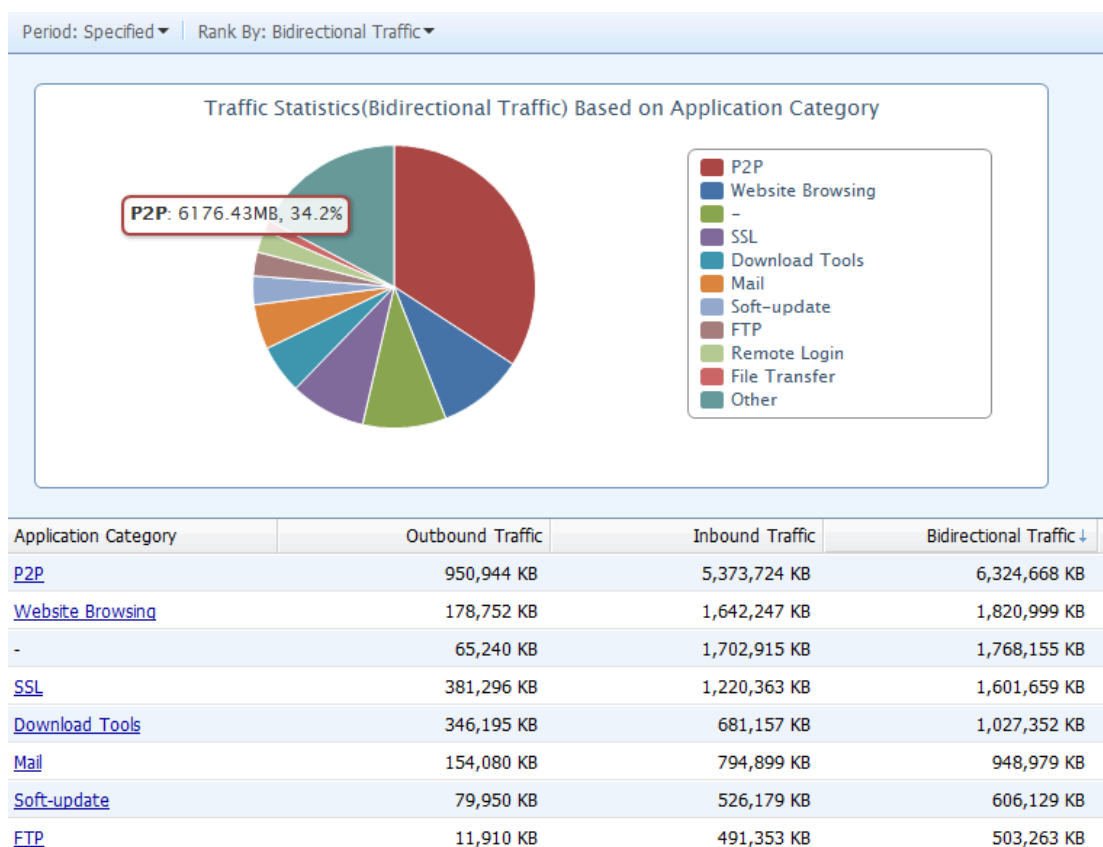
Period:
Specified
2013-08-12
-
2013-08-15
Schedule:
All week
IP/User:
All
Application:
All
Action:
Allow
Deny

Others

Statistics:
App Category
Application
IP/User
Show Top:
10
Less <<

Go
Open in new tab

Step 2: Click **Go**. Relevant data is generated.



The data shows that DNS applications have the highest access frequency among intranet users.



To enable the data center to collect application statistics, choose **Access Control > Application Control Policy**, create a policy, and click **Log event** in the **Action** area.

Website Browsing

The **Website Browsing** page enables users to collect statistics on the website browsing behavior of intranet users.

Example

Application scenario: A user needs to show the top 10 websites that are accessed by intranet users most frequently on May 30 so as to know the Internet behavior of intranet users.

Step 1: Set statistic criteria.

Website Browsing

Specify the following and click Go to retrieve data.

Filter

Period:
Specified
2013-08-12
-
2013-08-15

Schedule:
All week

IP/User:
All
IP
User
Group

URL Category:
All

Action:
Allow
Deny

Others

Statistics:
URL Category
Domain
IP/User

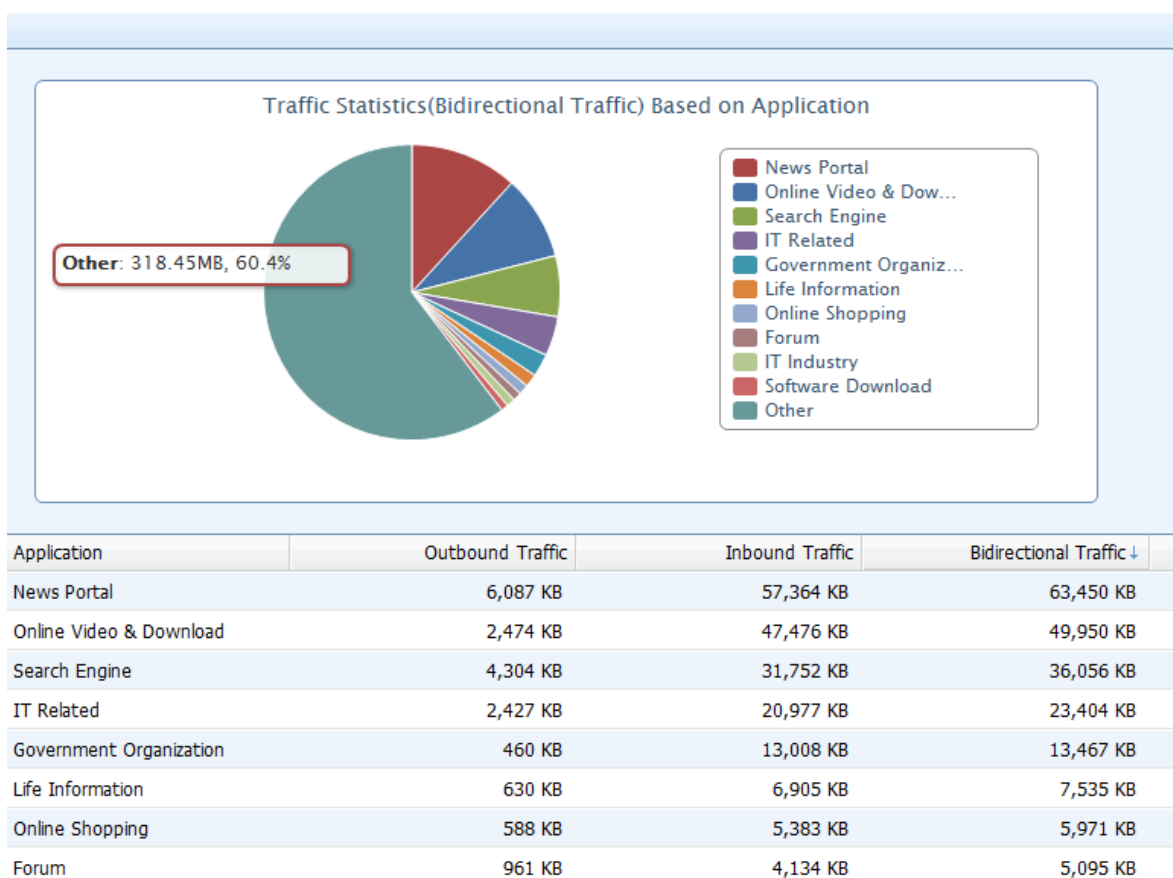
Rank By:
Access Count

Show Top:
10

Less <<

Go
Open in new tab

Step 2: Click **Go**. Relevant data is generated.



The data shows that news websites are accessed by intranet users most frequently.



To enable the data center to collect statistics on website browsing, go to **Intranet Security > Web Filter**, create a rule, and click **Log event** in the **Action** area.

Antivirus Statistics

The **Anti-Virus** page enables users to collect statistics on viruses that are found in **Intranet Security > Virus Defense and Filter**. For example, a user can identify the intranet user with the greatest number of viruses detected when sending or downloading files through FTP.

The screenshot shows the 'Anti-Virus' configuration page. At the top, there is a blue header with the text 'Anti-Virus'. Below the header, a message says 'Specify the following and click Go to retrieve data.' with a small bar chart icon. The page is divided into two main sections: 'Filter' and 'Others'. In the 'Filter' section, there are fields for 'Period' (set to 'Specified' with a dropdown arrow and date pickers for '2013-08-15' and '2013-08-15'), 'IP/User' (with radio buttons for 'All', 'IP', 'User', and 'Group', where 'All' is selected), 'Virus Type' (a dropdown menu set to 'All'), and 'Data Type' (with checkboxes for 'Sent' and 'Received', both of which are checked). In the 'Others' section, there are 'Statistics' radio buttons for 'Virus Name' (selected), 'Virus Type', and 'IP/User', and a 'Show Top' field set to '10' with a small table icon. At the bottom left of the form is a 'Less <<' link. At the bottom right, there is a 'Go' button and a checkbox labeled 'Open in new tab'.

Example

Application scenario: A user needs to show the top 10 intranet users with the greatest number of virus attacks when sending and receiving emails on May 30.

Step 1: Set statistic criteria.

Anti-Virus

Specify the following and click Go to retrieve data.

Filter

Period: -

IP/User: ☒ All ☐ IP ☐ User ☐ Group

Virus Type:

Data Type: ☒ Sent ☒ Received

Others

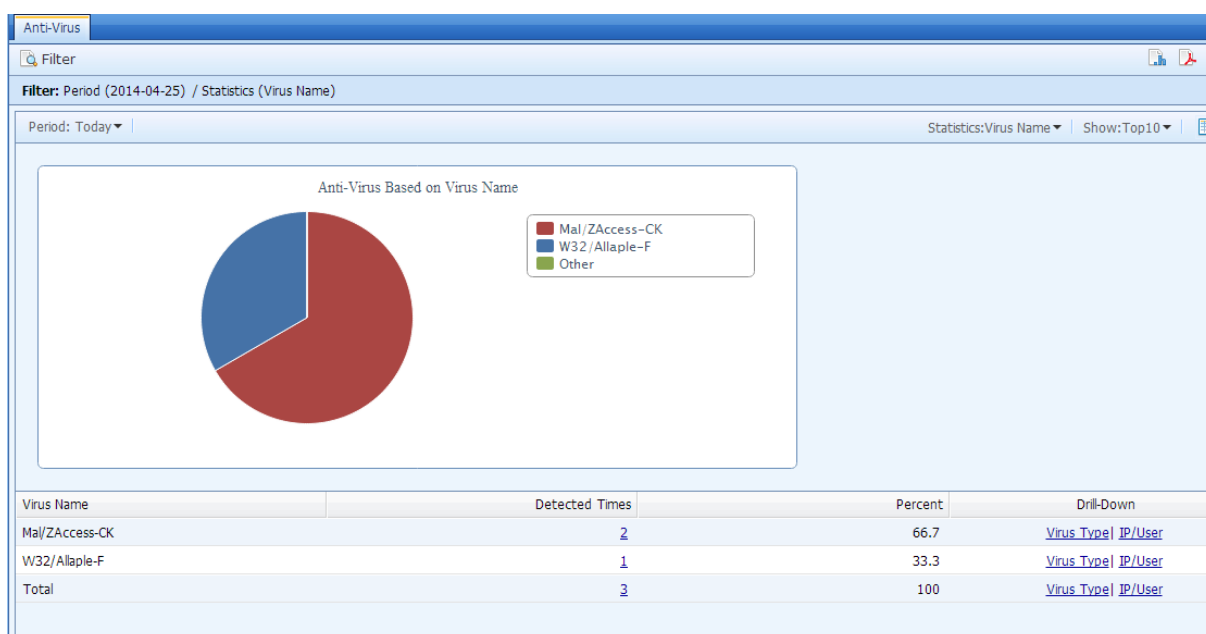
Statistics: ☒ Virus Name ☐ Virus Type ☐ IP/User

Show Top:

[Less <<](#)

☐ Open in new tab

Step 2: Click **Go**. Relevant data is generated.



The data shows that the firewall detected email viruses on the PC with the IP address 200.200.3.31 on May 30.



To enable the data center to collect antivirus statistics, click Log event in the Action area on the console; otherwise, no statistics are generated.

Logs

The **Logs** menu enables users to view log details. For example, a user can identify the server on the intranet that encounters a DoS attack, as well as the source IP address and port of the attack.

Navigation Menu <<

- Statistics
- ▼ **Logs**
 - DoS Attack
 - WAF
 - IPS
 - Anti-virus
 - APT Detection
 - Website Browsing
 - Application Control
 - Local Security Events
 - User Login/Logout
 - Admin Operation

DoS Attack

Specify the following and click Go to retrieve

From: 2014-09-05 15:00

To: 2014-09-05 15:00

Zone Type: ☒ Internal ☒ External

Source Zone: All

Src IP: All

Dst IP: All

Attack Type: All

Threat Level: ☒ High ☒ Medium


Action: ☒ Allow ☒ Deny

Go ☐ Open in new tab

DoS Attack

The **DoS Attack** page enables users to view details about DoS attacks on the intranet and Internet. For example, a user can view details about ICMP flood attacks on all servers on the intranet over a period.

DoS Attack

 Specify the following and click Go to retrieve data.

From:
2013-08-16
00:00

To:
2013-08-16
23:59

Zone Type:
☒ Internal
☒ External

Source Zone:
All

Source IP:
All

Dst IP:
All

Attack Type:
All

Threat Level:
☒ High
☒ Medium
☒ Low

Action:
☒ Allow
☒ Deny


Go
☐ Open in new tab

Example

Application scenario: A user needs to view details about the DoS attacks on intranet servers on May 30. The search excludes the DoS attacks on intranet users.

Step 1: Set search criteria. Set **Zone Type** to **External** because the search target is intranet servers.

DoS Attack

 Specify the following and click Go to retrieve data.

From:
2013-08-16
00:00

To:
2013-08-16
23:59

Zone Type:
☐ Internal
☒ External

Source Zone:
All

Source IP:
All

Dst IP:
All

Attack Type:
All

Threat Level:
☒ High
☒ Medium
☒ Low

Action:
☒ Allow
☒ Deny

Go
☐ Open in new tab

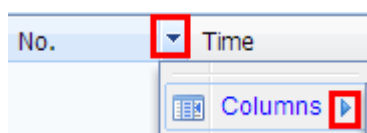
Step 2: Click **Go**. Relevant data is generated.

DoS Attack								
<div>Filter</div> <div>Export Logs</div>								
Filter: Period (2014-04-25 00:00~2014-04-25 23:59) Zone type(Internal,External) Src zone (All) Src IP (All) Dst IP (All) Type (All) Threat level (High,Medium,Low) Action (Allow,Deny)								
No.	Time	Type	Source IP	Dst IP	Description	Threat Level	Action	Details
1	2014-04-25 12:56:11	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
2	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	<div>No. 2</div> <div>Time: 2014-04-25 12:57:45</div> <div>Type: Sending IP fragment</div> <div>Src Zone: WAN</div> <div>Source IP: 192.200.19.200</div> <div>Dst IP: 192.200.19.63</div> <div>Policy Name: test</div> <div>Description: -</div> <div>Threat Level: Medium</div> <div>Action: Allow</div>			View	
3	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200				View	
4	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200				View	
5	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200				View	
6	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200				View	
7	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200				View	
8	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200				View	
9	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200				View	
10	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200				View	
11	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200				View	
12	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
13	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
14	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
15	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
16	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
17	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
18	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
19	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
20	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View
21	2014-04-25 12:57:45	Sending IP fragment	192.200.19.200	192.200.19.63	-	Medium	Allow	View

The data shows that the server with the IP address 200.200.2.101 on the intranet encounters a DoS attack from the Internet at 16:14, May 30. The attack type is IP data block fragmentation transmission and the source IP address of the attack is 58.60.9.178.



To display a certain column, click




in the upper right corner.

Web Application Protection

Web application protection enables users to view attacks detected in **Server Protection**.

WAF

 Specify the following and click Go to retrieve data.

From:

2013-08-01

15

00:00

To:

2013-08-16

15

23:59

Source Zone:

All

▼

Source IP:

All

i

Dst Zone:

All

▼

Dst IP:

All

i

Type:

All

▼

Rule ID:

All

i

State Code:

All

i

Threat Level:

☒ High

☒ Medium

☒ Low

Action:

☒ Allow

☒ Deny

Merge Logs:

☒ Enable

i

Go

☐ Open in new tab

Example

Application scenario: A user needs to view details about the SQL injection attacks sent by the client with the IP address 192.200.17.128 on August 16.

Step 1: Set search criteria.

Filter | Export Logs

Specify the following and click Go to retrieve data.

From: 2013-08-16 00:00

To: 2013-08-16 23:59

Source Zone: All

Source IP: 192.200.17.128

Dst Zone: All

Dst IP: All

Type: All

Rule ID: All

State Code: All

Threat Level: ☒ High ☒ Medium ☒ Low

Action: ☒ Allow ☒ Deny

Merge Logs: ☒ Enable

Go Cancel ☒ Open in new tab

Step 2: Click **Go**. Relevant data is generated.

WAF WAF *												
Filter Export Logs												
Filter: Period (2013-08-16 00:00~2013-08-16 23:59) Src zone (All) Src IP (192.200.17.128) Dst zone (All) Dst IP (All) Rule ID (All) State Code (All) Type (All) Device name () Threat lev												
No.	Time	Type	URL/Directory	Source IP	Dst IP	Rule ID	Desc...	Threat Level	Ac...	De...	Data...	Bypass
1	2013-08-16 10:10:14	Information di...	wilkie-const.com/	192.200.17.1...	108.162.203....	13070171	Web...	High	De...	Vi...	View	Auto Bypass
2	2013-08-16 10:10:14	Information di...	uchidabashi.com/	192.200.17.1...	119.18.217.1...	13070171	Web...	High	De...	Vi...	View	Auto Bypass
3	2013-08-16 10:09:20	Information di...	summerjazz.net/	192.200.17.1...	216.92.220.2...	13070171	Web...	High	De...	Vi...	View	Auto Bypass
4	2013-08-16 10:05:13	Information di...	instalelectric.com...	192.200.17.1...	200.58.111.99	13070171	Web...	High	De...	Vi...	View	Auto Bypass
5	2013-08-16 09:35:34	Information di...	star-nmrc.com/	192.200.17.1...	67.18.81.10	13070171	Web...	High	De...	Vi...	View	Auto Bypass
6	2013-08-16 09:20:10	Information di...	pbya.com/	192.200.17.1...	184.154.14.24	13070171	Web...	High	De...	Vi...	View	Auto Bypass
7	2013-08-16 09:00:16	Information	Information disclosure	192.200.17.1...	186.233.144....	13070171	Web...	High	De...	Vi...	View	Auto Bypass
8	2013-08-16 09:00:16	Information di...	zagros-group.net/	192.200.17.1...	212.71.249.1...	13070171	Web...	High	De...	Vi...	View	Auto Bypass
9	2013-08-16 09:00:16	Information di...	gigabit.com.pl/	192.200.17.1...	195.242.93.1...	13070171	Web...	High	De...	Vi...	View	Auto Bypass
10	2013-08-16 09:00:16	Information di...	envi.ro/	192.200.17.1...	173.254.28.87	13070171	Web...	High	De...	Vi...	View	Auto Bypass
11	2013-08-16 09:00:16	Information di...	gfr.com.au/	192.200.17.1...	103.9.64.130	13070171	Web...	High	De...	Vi...	View	Auto Bypass
12	2013-08-16 08:55:20	Information di...	kmr-net.com/	192.200.17.1...	153.127.249....	13070171	Web...	High	De...	Vi...	View	Auto Bypass
13	2013-08-16 08:53:54	Information di...	www.rea-soft.ru/	192.200.17.1...	185.12.94.222	13070171	Web...	High	De...	Vi...	View	Auto Bypass
14	2013-08-16 08:53:53	Information di...	mastechn.com/	192.200.17.1...	64.207.147.1...	13070171	Web...	High	De...	Vi...	View	Auto Bypass
15	2013-08-16 08:53:51	Information di...	coketh.com/	192.200.17.1...	59.106.13.131	13070171	Web...	High	De...	Vi...	View	Auto Bypass
16	2013-08-16 08:53:48	Information di...	bigtopmultimedia....	192.200.17.1...	217.115.114.4	13070171	Web...	High	De...	Vi...	View	Auto Bypass

Move the cursor to **Information** to show details.

No. 1

Time:	2013-08-16 10:10:14
Type:	Information disclosure
Protocol:	HTTP
Method:	POST
URL/Directory:	wilkie-const.com/
Src Zone:	LAN
Source IP:	192.200.17.128
Src Port:	55404
Dst Zone:	WAN_TEST
Dst IP:	108.162.203.130
Dst Port:	80
Rule ID:	13070171
State Code:	403
Policy Name:	CTI server
Description:	Website-based attack is detected. Type:Information disclosure
Threat Level:	High
Action:	Deny




To enable the data center to display logs, choose **Server Security > Web Application Protection** and click **Log event** in the **Action** area .

IPS

The **IPS** page enables users to view exploits of vulnerabilities detected by the IPS module.

IPS

 Specify the following and click Go to retrieve data.

From:

2013-08-16

15

00:00

To:

2013-08-16

15

23:59

Source Zone:

All

Source IP:

All

Dst Zone:

All

Dst IP:

All

Attack Type:

All

ID

All

Threat Level:

☒ High

☒ Medium

☒ Low

Action:

☒ Allow

☒ Deny

Go

☐ Open in new tab

Example

Application scenario: A user needs to view details about the exploits of server vulnerabilities mounted from the Internet to the intranet on May 30.

Step 1: Set search criteria.

Filter | Export Logs

Specify the following and click Go to retrieve data.

From: 2013-08-05 00:00

To: 2013-08-05 23:59

Source Zone: LAN

Source IP: All

Dst Zone: WAN_TEST

Dst IP: All

Attack Type: All

ID: All

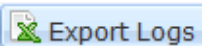

Threat Level: ☒ High ☒ Medium ☒ Low

Action: ☒ Allow ☒ Deny

Go Cancel ☒ Open in new tab

Step 2: Click **Go**. Statistics on IPS exploits of vulnerabilities mounted from the WAN to LAN are displayed.

Filter: Period (2013-08-05 00:00~2013-08-05 23:59) Src zone (LAN) Src IP (All) Dst zone (WAN_TEST) Dst IP (All) Attack type (All) ID (All) Device name () Threat level (High,Medium,Low)												
No.	Time	Type	Source IP	Dst IP	ID	Name	Description	Reference	Threat	Action	Details	
1	2013-08-05 16:15:31	system	172.16.2.2	172.16.2.3	10010...	DOS Gewse	Could lead to a loss o...	-	Medium	Allow	View	
2	2013-08-05 16:15:31	web	172.16.2.2	172.16.2.3	11020...	OpenSSL SSLv2...	The issue occurs in t...	http://www.securityf...	Medium	Allow	View	
3	2013-08-05 16:15:31	web	172.16.2.2	172.16.2.3	11020...	OpenSSL SSLv2...	The issue occurs in t...	http://www.securityf...	Medium	Allow	View	
4	2013-08-05 16:15:31	system	172.16.2.2	172.16.2.3	10010...	X-Scan Services ...	This event indicates t...	-	Medium	Allow	View	
5	2013-08-05 16:12:47	system	172.16.2.2	172.16.2.3	10010...	Microsoft Windo...	Microsoft Windows 2...	http://www.securityf...	Medium	Allow	View	
6	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	
7	2013-08-05 16:12:47	system	172.16.2.2	172.16.2.3	10010...	Linux Vendor rp...	rpc.statd in the nfs-u...	http://www.securityf...	High	Deny	View	
8	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	
9	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	
10	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	
11	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	
12	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	
13	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	
14	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	
15	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	
16	2013-08-05 16:12:47	mail	172.16.2.2	172.16.2.3	2087	Sendmail Heade...	A vulnerability exists i...	http://www.securityf...	High	Deny	View	

Click  in the upper left corner to export the data to an EXCEL file. Click  in the upper right corner to display a certain column.



To enable the data center to record logs, create a rule on the IPS page of the console and click Log event following Logging in the Action area.

Anti-virus

The **Anti-Virus** page enables users to view logs of viruses detected in **Access Control > Anti-Virus**.

Anti-virus

Filter | Export Logs

Specify the following and click Go to retrieve data.

From: 2013-08-01 00:00

To: 2013-08-16 23:59

Source Zone: All

Src IP/User: ☒ All ☐ IP ☐ User ☐ Group

Dst Zone: All

Application: All

Data Type: ☒ Sent ☒ Received

Go Cancel ☒ Open in new tab

Example

Application scenario: A user needs to view details about virus scanning and removal when emails are sent or received from the intranet to the Internet on May 30.

Step 1: Set search criteria.

Anti-virus

Filter | Export Logs

Specify the following and click Go to retrieve data.

From: 2013-08-01 00:00

To: 2013-08-16 23:59

Source Zone: LAN

Src IP/User: ☒ All ☐ IP ☐ User ☐ Group

Dst Zone: WAN

Application: Email

Go Cancel ☒ Open in new tab

Step 2: Click **Go**. Data that meets the search criteria is displayed.

Anti-Virus								
Anti-Virus Details								
Export Logs								
Filter: Period (2014-04-25 00:00~2014-04-25 23:59) Src zone (All) Src IP/user (All) Dst zone (All) Application (All) Action (Sent,Received)								
No.	Time	Behavior	File Name	Virus Name	Source IP/User	Address	Action	Details
1	2014-04-25 14:53:23	EmailReceived	/fwlog/mailproxy/pop...	Mal/ZAccess-CK	192.200.19.63	kwong@sangfortest.com	Allow	View
2	2014-04-25 14:53:03	EmailSent	/fwlog/mailproxy/smt...	Mal/ZAccess-CK	192.200.19.63	kwong@sangfortest.com	Allow	View

The data shows that a sent email containing a virus is allowed.



To enable the data center to record logs, choose **Access Control > Anti-Virus** on the console, create a rule, and click **Log event** following **Logging** in the **Action** area.

APT Detection

The **APT Detection** page enables users to view logs of APT detected in **Access Control > APT Detection**.

APT Detection

Specify the following and click Go to retrieve data.

From: 2014-09-01 00:00

To: 2014-09-05 23:59

Source Zone: All

Src IP/User: ☒ All ☐ IP ☐ User ☐ Group

Dst Zone: All

Type: All

ID: All

Threat Level: ☒ High ☒ Medium ☒ Low

Action: ☒ Allow ☒ Deny

Go ☐ Open in new tab

Example

Application scenario: A user needs to search for the IP addresses or users on the intranet that generate APT traffic.

Step 1: Set search criteria.

APT Detection

Specify the following and click Go to retrieve data.

From: 2014-09-01 00:00

To: 2014-09-05 23:59

Source Zone: All

Src IP/User: ☒ All ☐ IP ☐ User ☐ Group

Dst Zone: All

Type: All

ID: All

Threat Level: ☒ High ☒ Medium ☒ Low

Action: ☒ Allow ☒ Deny

Go ☐ Open in new tab

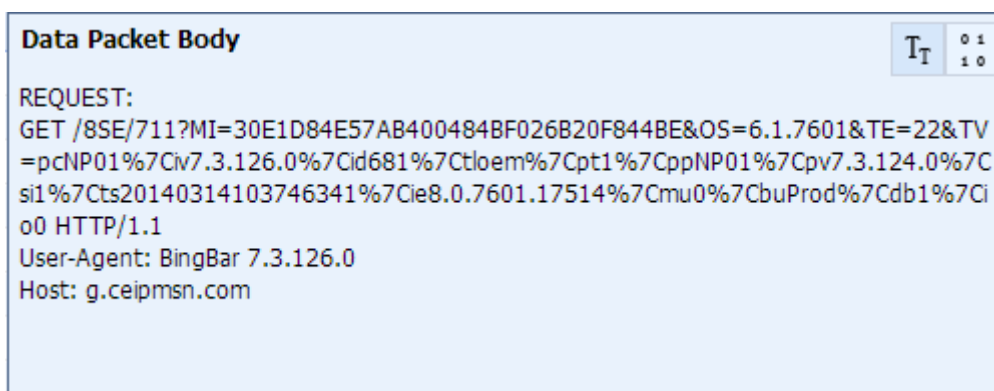
Step 2: Click **Go**. Data that meets the search criteria is displayed.

Anti-Malware									
Filter Export Logs									
Filter: Period (2014-03-03 00:00~2014-03-20 23:59) Src zone (All) Src IP/user (All) Dst zone (All) ID(All) Type (All) Threat level (High,Medium,Low) Action (Allow,Deny)									
No.	Time	Type	Source IP/User	Dst IP	Action	Description	Details	Data Pa...	Bypass
1	2014-03-14 18:35:58	Botnet	10.0.0.2	131.253.40.10	Deny	The host 10.0.0.2 may be infected B...	View	View	Auto Bypass
2	2014-03-14 18:24:37	Botnet	10.0.0.2	131.253.40.10	Deny	The host 10.0.0.2 may be infected B...	View	View	Auto Bypass
3	2014-03-14 18:22:50	Botnet	10.0.0.2	157.55.34.242	Deny	The host 10.0.0.2 may be infected B...	View	View	Auto Bypass
4	2014-03-14 18:14:32	Botnet	10.0.0.2	157.55.34.242	Deny	The host 10.0.0.2 may be infected B...	View	View	Auto Bypass
5	2014-03-13 18:48:13	Botnet	10.0.0.2	131.253.40.10	Deny	The host 10.0.0.2 may be infected B...	View	View	Auto Bypass
6	2014-03-13 18:12:12	Botnet	10.0.0.2	157.56.229.209	Deny	The host 10.0.0.2 may be infected B...	View	View	Auto Bypass
7	2014-03-13 17:38:18	Botnet	10.0.0.2	131.253.40.10	Deny	The host 10.0.0.2 may be infected B...	View	View	Auto Bypass

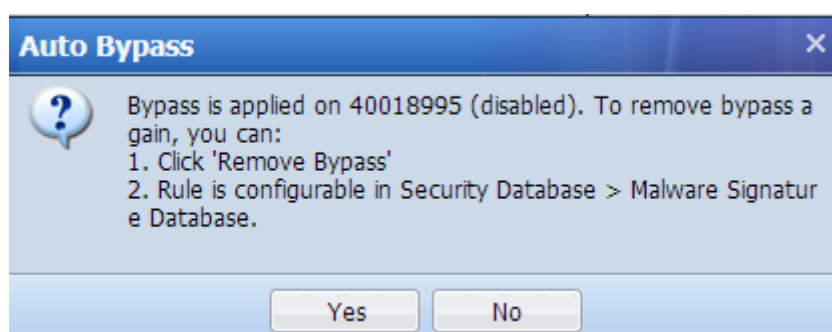
Step 3: Click **Details** to view the information that matches the APT policy.



Step 4: Click **Data Packet** to view the packet that matches the APT policy.



Step 5: Click **Auto Bypass** to disable the rule for matching the Botnet feature database. The function is used when the administrator finds misvaluation.



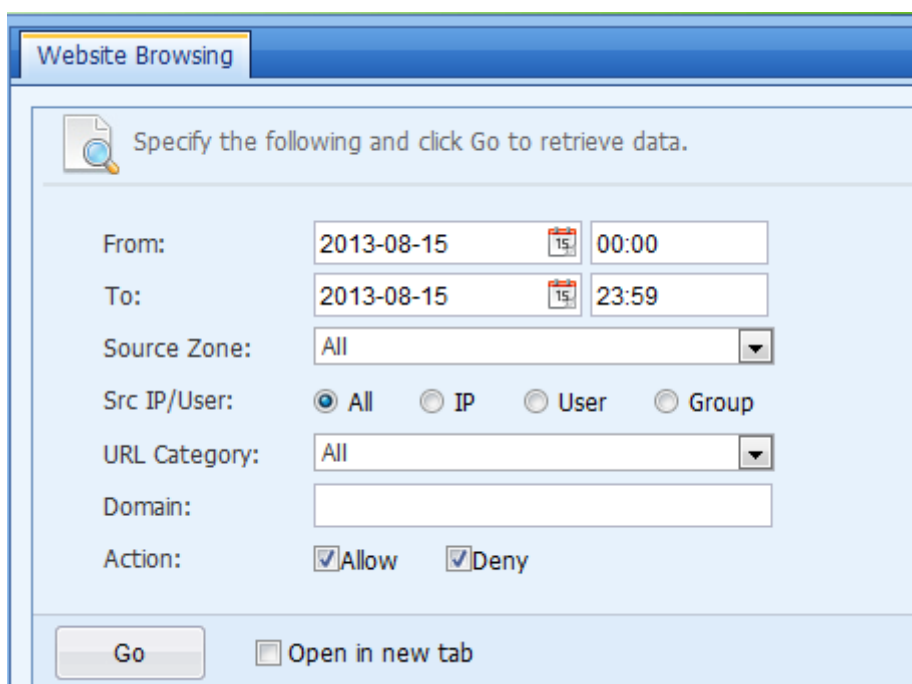
Website Browsing

The **Website Browsing** page enables users to view details about the website browsing behavior of intranet users. For example, a user can search for the URLs accessed by an IP address on the intranet on a day. The following figure shows the **Website Browsing** page.

Example

Application scenario: A user needs to search for all websites accessed by the source IP address 200.200.2.51 on May 30.

Step 1: Set search criteria.



The screenshot shows a web application window titled "Website Browsing". Inside, there is a search form with the instruction "Specify the following and click Go to retrieve data." The form includes the following fields and options:

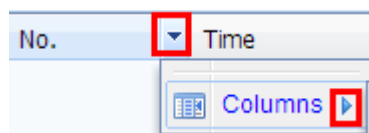
- From:** A date and time selector set to "2013-08-15" and "00:00".
- To:** A date and time selector set to "2013-08-15" and "23:59".
- Source Zone:** A dropdown menu currently showing "All".
- Src IP/User:** Radio buttons for "All" (selected), "IP", "User", and "Group".
- URL Category:** A dropdown menu currently showing "All".
- Domain:** An empty text input field.
- Action:** Checkboxes for "Allow" and "Deny", both of which are checked.

At the bottom of the form, there is a "Go" button and a checkbox labeled "Open in new tab".

Step 2: Click **Go**. Data that meets the search criteria is generated.

Website Browsing							
Filter		Export Logs					
Filter: Period (2014-04-25 00:00~2014-04-25 23:59) Src zone (All) Src IP/user (All) Action (Allow,Deny) URL category (All) Domain ()							
No.	Time	URL Category	Domain	URL	Source IP/User	Action	Details
10	2014-04-25 12:59:27	Other	sjc-login.dotomi.com	sjc-login.dotomi.com/commonid...	192.200.19.63	Allow	View
11	2014-04-25 12:59:25	Other	https://secure-ds.serving-sys.com	https://secure-ds.serving-sys.com	192.200.19.63	Allow	View
12	2014-04-25 12:59:25	Other	https://secure-ds.serving-sys.com	https://secure-ds.serving-sys.com	192.200.19.63	Allow	View
13	2014-04-25 12:59:25	Other	https://secure-ds.serving-sys.com	https://secure-ds.serving-sys.com	192.200.19.63	Allow	View
14	2014-04-25 12:59:25	Other	media.fastclick.net	media.fastclick.net/w/get.medi...	192.200.19.63	Allow	View
15	2014-04-25 12:59:23	Advertisement	googleads.g.doubleclick.net	googleads.g.doubleclick.net/pa...	192.200.19.63	Allow	View
16	2014-04-25 12:58:53	Other	https://10.1.7.250	https://10.1.7.250	192.200.19.63	Allow	View
17	2014-04-25 12:58:51	Advertisement	ad.doubleclick.net	ad.doubleclick.net/activity;src=...	192.200.19.63	Allow	View
18	2014-04-25 12:58:45	Other	ib.adnxs.com	ib.adnxs.com/mapuid?member=...	192.200.19.63	Allow	View
19	2014-04-25 12:58:43	Search Engine	https://google.com	https://google.com	192.200.19.63	Allow	View
20	2014-04-25 12:58:43	Other Enterprise Website	b.scorecardresearch.com	b.scorecardresearch.com/p?c1...	192.200.19.63	Allow	View
21	2014-04-25 12:58:43	Adult Content	ds.serving-sys.com	ds.serving-sys.com/burstingres/...	192.200.19.63	Allow	View
22	2014-04-25 12:58:43	Other Enterprise Website	my.gmads.mookie1.com	my.gmads.mookie1.com/247?g...	192.200.19.63	Allow	View
23	2014-04-25 12:58:43	Other	n.effectivevmeasure.net	n.effectivevmeasure.net/emmb_...	192.200.19.63	Allow	View
24	2014-04-25 12:58:43	Other	a.tribalfusion.com	a.tribalfusion.com/p.media/a0m...	192.200.19.63	Allow	View
25	2014-04-25 12:58:43	Other	themes.googleusercontent.com	themes.googleusercontent.co...	192.200.19.63	Allow	View
26	2014-04-25 12:58:43	Life Information	bs.serving-sys.com	bs.serving-sys.com/burstingppe...	192.200.19.63	Allow	View
27	2014-04-25 12:58:43	Search Engine	fonts.googleapis.com	fonts.googleapis.com/css?family...	192.200.19.63	Allow	View
28	2014-04-25 12:58:43	IT Related	www.gstatic.com	www.gstatic.com/doubleclick/s...	192.200.19.63	Allow	View
29	2014-04-25 12:58:41	Search Engine	https://accounts.google.com	https://accounts.google.com	192.200.19.63	Allow	View
30	2014-04-25 12:58:41	Advertisement	https://ad.doubleclick.net	https://ad.doubleclick.net	192.200.19.63	Allow	View

Click  **Export Logs** in the upper left corner to export the data to an EXCEL file. Click




in the upper right corner to display a certain column.

Application Control

The **Application Control** page enables users to view the logs generated in **Access Control > Application Control Policy**.

Application Control

 Specify the following and click Go to retrieve data.

From: 2013-08-15 00:00

To: 2013-08-15 23:59

Source Zone: All

Src IP/User: ☒ All ☐ IP ☐ User ☐ Group

Dst Zone: All

Dst IP: All

Service/Application: All

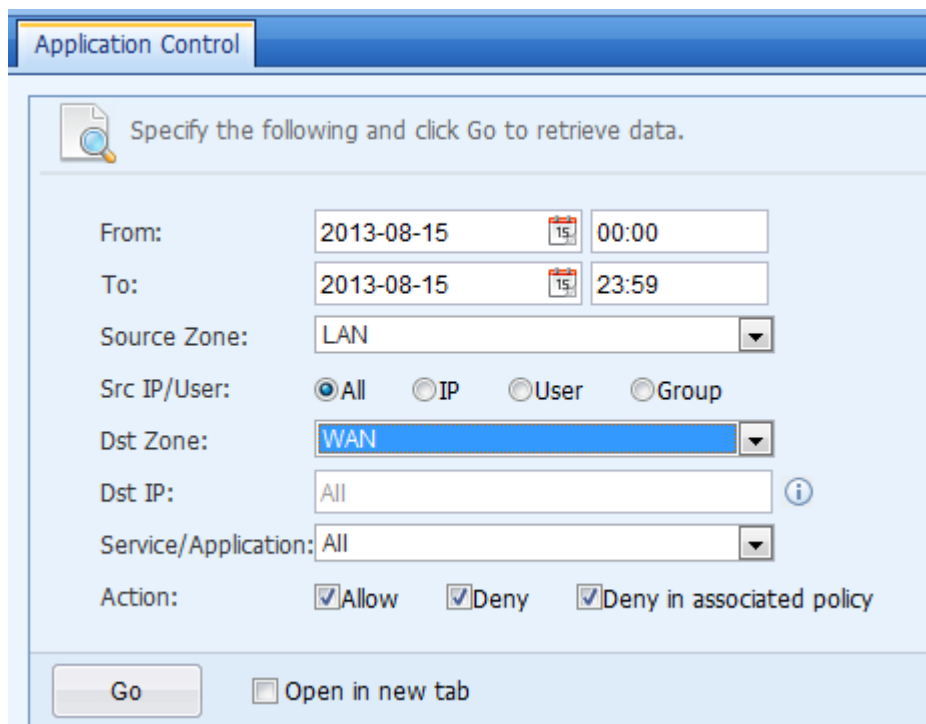
Action: ☒ Allow ☒ Deny ☒ Deny in associated policy

Go ☐ Open in new tab

Example

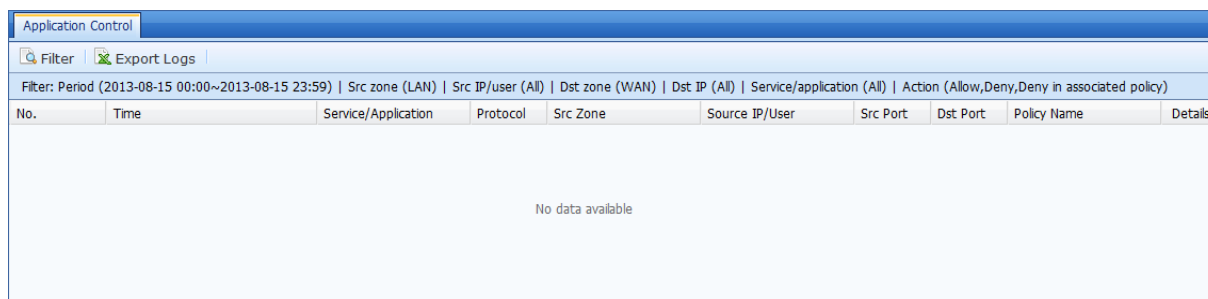
Application scenario: A user needs to view the logs concerning the traffic from the LAN to WAN that is denied by the application control policy on May 30.

Step 1: Set search criteria.



The screenshot shows the 'Application Control' search interface. It includes fields for 'From' and 'To' dates and times, 'Source Zone' (LAN), 'Src IP/User' (All, IP, User, Group), 'Dst Zone' (WAN), 'Dst IP' (All), 'Service/Application' (All), and 'Action' (Allow, Deny, Deny in associated policy). A 'Go' button and an 'Open in new tab' checkbox are at the bottom.

Step 2: Click **Go**. Data that meets the search criteria is displayed.




The screenshot shows the search results table. The filter bar at the top indicates the search criteria: Period (2013-08-15 00:00~2013-08-15 23:59) | Src zone (LAN) | Src IP/user (All) | Dst zone (WAN) | Dst IP (All) | Service/application (All) | Action (Allow,Deny,Deny in associated policy). The table has columns for No., Time, Service/Application, Protocol, Src Zone, Source IP/User, Src Port, Dst Port, Policy Name, and Details. The table is currently empty, displaying 'No data available'.

No.	Time	Service/Application	Protocol	Src Zone	Source IP/User	Src Port	Dst Port	Policy Name	Details
No data available									

Local Security Event

The **Local Security Event** page shows the overall security event of the local network which enable user to view the security issues happened in the network.

Local Security Events

 Specify the following and click Go to retrieve data.

From: 2014-08-01 00:00
 To: 2014-09-05 23:59
 Source Zone: All
 Src IP: All
 Attack Type: All
 Threat Level: ☒ High ☒ Medium ☒ Low
 Action: ☒ Allow ☒ Deny


Go ☐ Open in new tab

Example

Application scenario: A user needs to view the logs concerning the traffic from the LAN to WAN that is denied by the application control policy on September 30.

Step 1: Set search criteria.

Local Security Events


 Specify the following and click Go to retrieve data.

From: 2014-08-01 00:00
 To: 2014-09-30 23:59
 Source Zone: All
 Src IP: All
 Attack Type: All
 Threat Level: ☒ High ☒ Medium ☒ Low
 Action: ☒ Allow ☒ Deny

Go ☐ Open in new tab

Step 2: Click **Go**. Data that meets the search criteria is displayed.

Local Security Events

 Filter

 Export Logs


Filter: Period (2014-08-01 00:00~2014-09-30 23:59) | Src zone (All) | Src IP (All) | Type (All) | Threat level (High,Medium,Low) | Action (Allow,Deny)

No.	Date	Type	Source IP	Description	Threat Level	Action	Details

User Login/Logout

The **User Login/Logout** page enables users to view the login and logout information of common users that are successfully authenticated by the authentication module of the NGAF. For example, a user can search for the users that log in and out from 12:00 to 13:00 on a certain day.

User Login/Logout

 Specify the following and click Go to retrieve data.

From:

2013-08-15

00:00

To:

2013-08-15

23:59

Src IP/User:

☒ All
☐ IP
☐ User
☐ Group

Go


☐ Open in new tab

Example

Application scenario: A user needs to find whether the source IP address 192.200.17.10 is successfully authenticated by the authentication module of the NGAF on August 15.

Step 1: Set search criteria.

User Login/Logout

 Specify the following and click Go to retrieve data.

From:

2013-08-15

00:00

To:


2013-08-15

23:59

Src IP/User:

☐ All
☒ IP
☐ User
☐ Group

192.200.17.10



Go

☐ Open in new tab

Step 2: Click **Go**. Data that meets the search criteria is generated.

User Login/Logout

Filter

Export Logs

Filter: Period (2013-08-15 00:00~2013-08-15 23:59) | Src IP/user (IP:192.200.17.10)


No.	Username	Group	Login IP	Last Login	Last Logout	Online Duration	Details
1	sangfor	/	192.200.17.10	2013-08-15 08:24:03	2013-08-15 20:36:03	12 hours 12 minutes	<div><div>No. 1</div><div><div>Username: sangfor</div><div>Group: /</div><div>Login IP: 192.200.17.10</div><div>Last Login: 2013-08-15 08:24:03</div><div>Last Logout: 2013-08-15 20:36:03</div><div>Online Duration: 12 hours 12 minutes</div></div></div> <div>View</div>

The data shows that the source IP address 200.200.2.113 was successfully authenticated by the authentication module of the NGAF on May 30 and stayed online for 10 hours, 52 minutes and 9 seconds.

Admin Operation

The **Admin Operation** page enables users to view the logs generated throughout the process whereby a user logs in to the console, performs operations, and then logs out. For example, a user can view the logs concerning the operations performed on the console by the account **admin** after login. The following figure shows the **Admin Operation** page.


Admin Operation



Specify the following and click Go to retrieve data.

From:


2013-08-15



00:00

To:


2013-08-15



23:59

Admin:

All



Description:

Go

☐ Open in new tab

Example

Application scenario: A user needs to view the logs concerning the operations performed on the console by the account **admin** after login on August 15.

Step 1: Set search criteria.

Admin Operation

Specify the following and click Go to retrieve data.

From: 2013-08-15 00:00

To: 2013-08-15 23:59

Admin: All

Description:

☐ Open in new tab

Step 2: Click **Go**. Data that meets the search criteria is generated.

Admin Operation							
Filter: Period (2013-08-15 00:00~2013-08-15 23:59) User (All) Description ()							
No.	Username	Host IP	Target	Operation	Time	Details	
1	admin	192.200.17.10	Report center	No. 1 Username: admin Host IP: 192.200.17.10 Target: Report center Operation: Log In Time: 2013-08-15 16:57:49 Description: admin 192.200.17.10 Log In successfully		View	
2	admin	192.200.17.10	Report center			View	
3	admin	192.200.17.10	Report center			View	
4	admin	192.200.17.10	Update			View	
5	admin	192.200.17.10	User logout			View	
6	admin	192.200.17.10	User login			View	
7	admin	192.200.17.10	Email alarm			View	
8	admin	192.200.17.10	High Availability > Redundancy	Disable	2013-08-15 14:43:33	View	
9	admin	192.200.17.10	High Availability > Redundancy	Enable	2013-08-15 14:42:39	View	
10	admin	192.200.17.10	High Availability	Modify basic settings	2013-08-15 14:42:34	View	
11	admin	192.200.17.10	Physical Interface	Modify settings	2013-08-15 14:41:12	View	
12	admin	192.200.17.10	Network > Interface > Zone	Modify	2013-08-15 14:41:12	View	
13	admin	192.200.17.10	Administrator account	Add	2013-08-15 14:34:51	View	
14	admin	192.200.17.10	User logout	Log out	2013-08-15 14:19:56	View	
15	admin	192.200.17.10	User login	Log In	2013-08-15 14:19:56	View	
16	admin	192.200.17.10	Exclusion Rule	Add exclusion rule	2013-08-15 12:32:30	View	

Statistics Report

The Statistics Report module is used to set custom reports, search for statistic reports, and subscribe to reports. It consists of the Reports, Custom Report, and Subscription submodules.

Reports

The **Reports** page enables users to search for statistic reports and the reports generated on the **Subscription** and **Custom Report** pages.

Reports

Specify the following and click Go to retrieve data.

Period: 2012-08-16 - 2013-08-16

Report Type: All

Report Name:

Go

Set **Period**, **Report Type**, and **Report Name**, and click **Go**. Data that meets the search criteria is displayed.

Report Name	Report Type	Generated	User	Operation
Custom_Report	Custom report	2013-08-16 10:52:16	admin	Export as PDF File Send Mail

The searched reports can be exported to a PDF file, sent as emails, or deleted.

Custom Report

The **Custom Report** page enables users to customize reports based on required information.

Custom Report

Report Name: Custom_Report

Filter

Period: 2013-08-16 - 2013-08-16
Schedule: All week
IP/User: ☒ All ☐ IP ☐ Group
Statistics Type: ☒ Ranking ☐ Trend ☐ Ranking & Trend
Show Top: 10

Report Contents

Report Type: Simplified report Full report

☒ Security
Type: ☒ Overall Security ☒ Server Security ☒ Endpoint Security
Threat Level: ☒ High ☒ Medium ☒ Low

☒ Traffic
Rank By: ☒ Bidirectional Traffic ☐ Outbound Traffic ☐ Inbound Traffic
Statistics: ☒ Application ☐ App Category ☐ Group ☐ IP/User
App Category: All

☒ Application
Statistics: ☒ Application ☐ App Category ☐ IP/User
App Category: All

☒ Website Browsing

Example

Application scenario: A user needs to customize a report that ranks all websites accessed by intranet users on May 30 by access frequency. Other information is not required. The report must be generated in the NGAF so that it can be viewed on the **Reports** page.

Step 1: Click **Custom Report** and set statistic criteria.

Custom Report

Report Name: Custom_Report

Filter

Period: 2013-08-16 - 2013-08-16

Schedule: All week

IP/User: ☒ All ☐ IP ☐ Group

Statistics Type: ☒ Ranking ☐ Trend ☐ Ranking & Trend

Show Top: 10

Step 2: Select **Website Browsing** in the **Report Contents** area and set **Rank by** and **Statistics**.

Report Contents

Report Type:

Simplified report

Full report

Security

Type:

Overall Security

Server Security

Endpoint Security

Threat Level:

High

Medium

Low

Traffic

Rank By:

Bidirectional Traffic

Outbound Traffic

Inbound Traffic

Statistics:

Application

App Category

Group

IP/User

App Category:

All

Application

Statistics:

Application

App Category

IP/User

App Category:

All

Website Browsing

Rank By:

Bidirectional Traffic

Access Count

Block Count

Statistics:

Category

Domain

IP/User

Report File Format

Open on webpage (and saved to report list)

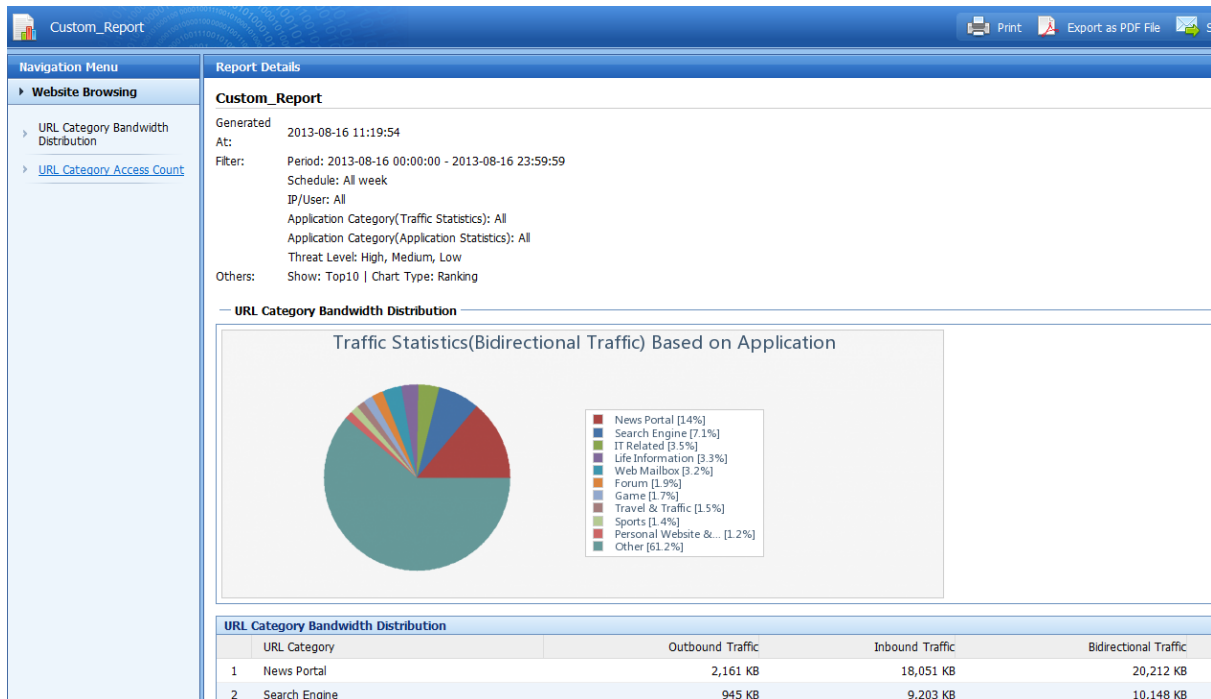
Save as PDF file (on local PC)

OK

Step 2: Click **OK**. A report that meets the criteria is generated.

SANGFOR NGAF 6.4 User Manual

404



Custom reports are one-off reports and cannot be generated repeatedly.

Subscription

The **Subscription** page enables users to generate periodic reports and send generated reports to specified mailboxes regularly.

Subscription

☒ Enable

Report Name:

Filter

Schedule:

IP/User: ☒ All ☐ IP ☐ Group

Statistics Type: ☒ Ranking ☐ Trend ☐ Ranking & Trend

Show Top:

Report Contents

Report Type: [Simplified report](#) [Full report](#)

☒ Security

Type: ☒ Overall Security ☒ Server Security ☒ Endpoint Security

Threat Level: ☒ High ☒ Medium ☒ Low

☒ Traffic

Rank By: ☒ Bidirectional Traffic ☐ Outbound Traffic ☐ Inbound Traffic

Statistics: ☒ Application ☐ App Category ☐ Group ☐ IP/User

App Category:

☒ Application

Statistics: ☒ Application ☐ App Category ☐ IP/User

App Category:

☒ Website Browsing

Rank By: ☒ Bidirectional Traffic ☒ Access Count ☐ Block Count

Statistics: ☒ Category ☐ Domain ☐ IP/User

Report Subscription

Periodic: ☒ Daily ☐ Weekly ☐ Monthly

Report Delivery: ☒ Save report but not send to me

☐ Send report to the following address (addresses are separated by semicolon)

Example

Application scenario: A user needs to subscribe to a report that collects statistics on the total traffic of all intranet users and ranks uplink and downlink traffic. The report collects statistics once every week and is sent from sangfor@sangfor.com to administrator@***.com.

Step 1: Configure an email server on the **Settings** page before setting report subscription. Set **Server Address**, **Username**, **Password**, and **Sender Address** (sangfor@sangfor.com) for the SMTP server corresponding to sangfor@sangfor.com.

The screenshot shows a 'Settings' window with a tab labeled 'SMTP Server'. The configuration fields are as follows:

- SMTP Server** (checked checkbox)
- Server Address:** 211.152.1.45
- Require authentication:** (checked checkbox)
- Username:** sangfor
- Password:** (masked with three dots)
- Sender Address:** sangfor@sangfor.com

Step 2: Click **Add** and select **Traffic** on the **Subscription** page. Leave other options unselected.

The screenshot shows a 'Subscription' window with a tab labeled 'Settings'. The configuration is as follows:

- Enable** (checked checkbox)
- Report Name:** Report
- Filter**
 - Schedule:** All week
 - IP/User:** All (selected), IP, Group
 - Statistics Type:** Ranking (selected), Trend, Ranking & Trend
 - Show Top:** 10
- Report Contents**
 - Report Type:** Simplified report, Full report
 - Security** (unchecked)
 - Type: Overall Security, Server Security, Endpoint Security
 - Threat Level: High, Medium, Low
 - Traffic** (checked)
 - Rank By: Bidirectional Traffic (checked), Outbound Traffic, Inbound Traffic
 - Statistics: Application (checked), App Category, Group, IP/User
 - App Category: All
 - Application** (unchecked)
 - Statistics: Application, App Category, IP/User
 - App Category: All
 - Website Browsing** (unchecked)
 - Rank By: Bidirectional Traffic, Access Count, Block Count
 - Statistics: Category, Domain, IP/User
- Report Subscription**
 - Periodic:** Daily, Weekly (selected), Monthly
 - Report Delivery:** Save report but not send to me, Send report to the following address (selected)
 - Address: administrator@abc.com (addresses are separated by semicolon)
 - Message: Unable to send email. SMTP server has not been configured. [SMTP Server](#)

Buttons: OK, Cancel

Step 3: Click **OK**.

Subscription									
Settings									
+ Add X Delete ✓ Enable ✗ Disable									
Report Name	Number of Reports	Last Generated	Email To	Periodic	Created By	Status	Operation		
Report	0	-	administrator@abc.com	Weekly	admin	✓	Generate		

System

The **System** menu enables users to configure settings related to the data center, such as setting the report generation time (precise to minutes), number of exported logs, and timeout time, or deleting logs.

Settings

☒ SMTP Server

Server Address:

11.1.1.1

☐ Require authentication

Sender Address:

sangfor@sangfor.com

Report Automatic Generation/Deletion

Generation Time:

00:00 - 06:00

Auto Deletion:

☒ Delete reports generated 7 days ago
☐ Preserve maximum 1000 newest reports

Log Lookup/Export

Log Export:

Export the latest 1000 logs by default

Lookup Capacity:

10000000

Restore Defaults

Miscellaneous

Idle Timeout:

10 minute(s)

Unit of Speed:

☒ bps
☐ Bps

OK

Settings

Click **Settings**. The **Settings** page is displayed.

The screenshot shows a 'Settings' window with the following sections:

- SMTP Server** (checked):
 - Server Address: 11.1.1.1
 - ☐ Require authentication
 - Sender Address: sangfor@sangfor.com
- Report Automatic Generation/Deletion**:
 - Generation Time: 00:00 - 06:00 (with info icon)
 - Auto Deletion:
 - ☒ Delete reports generated 7 days ago
 - ☐ Preserve maximum 1000 newest reports
- Log Lookup/Export**:
 - Log Export: Export the latest 1000 logs by default (with info icon)
 - Lookup Capacity: 10000000 (with 'Restore Defaults' link and info icon)
- Miscellaneous**:
 - Idle Timeout: 10 minute(s)
 - Unit of Speed: ☒ bps ☐ Bps

An 'OK' button is located at the bottom left of the window.

SMTP Server: is applicable when a user configures an email server in section 4.3.3.

Report Automatic Generation/Deletion: specifies the time when reports that are configured in section 4.3 are generated. The report storage time can also be specified.

Log Lookup/Export: specifies the maximum number of exported reports and that of displayed reports. The maximum values are not used by default to limit device performance consumption.

Miscellaneous: specifies the timeout time and traffic rate unit on the home page of the data center.

Log Database

The **Log Database** page enables users to view the sizes of logs generated over a specified period and perform related operations such as deleting logs.

The screenshot shows the 'Log Database' interface. On the left is a 'Navigation Menu' with options: Statistics, Logs, Statistics Reports, and System (expanded). Under 'System', there are 'Settings' and 'Log Database' (highlighted in red). The main area has a 'Log Database' tab. Below the tab, there is a search instruction: 'Specify the following and click Go to retrieve data.' Below this, there is a 'Period:' label followed by two date pickers: '2012-08-16' and '2013-08-16', separated by a minus sign. A 'Go' button is located below the date pickers.

Set the search period and click **Go**. The search result shows logs that are generated over the specified period.

The screenshot shows the search results for the Log Database. At the top, there is a 'Filter' button and a 'Delete' button. Below them, a 'Filter: Period (2012-08-01~2013-08-16)' is displayed. The table has two columns: 'Date' and 'Data Size'. The table contains 11 rows of data, each with a checkbox in the 'Date' column and the corresponding 'Data Size' in the 'Data Size' column.

Date	Data Size
<input type="checkbox"/> 20130805	1,700 KB
<input type="checkbox"/> 20130806	30,433 KB
<input type="checkbox"/> 20130807	96,596 KB
<input type="checkbox"/> 20130808	5,961 KB
<input type="checkbox"/> 20130809	6,000 KB
<input type="checkbox"/> 20130810	5,922 KB
<input type="checkbox"/> 20130811	5,993 KB
<input type="checkbox"/> 20130812	133,346 KB
<input type="checkbox"/> 20130813	124,354 KB
<input type="checkbox"/> 20130814	137,624 KB
<input type="checkbox"/> 20130815	113,718 KB

Click a date and click . Logs generated on the day are deleted.



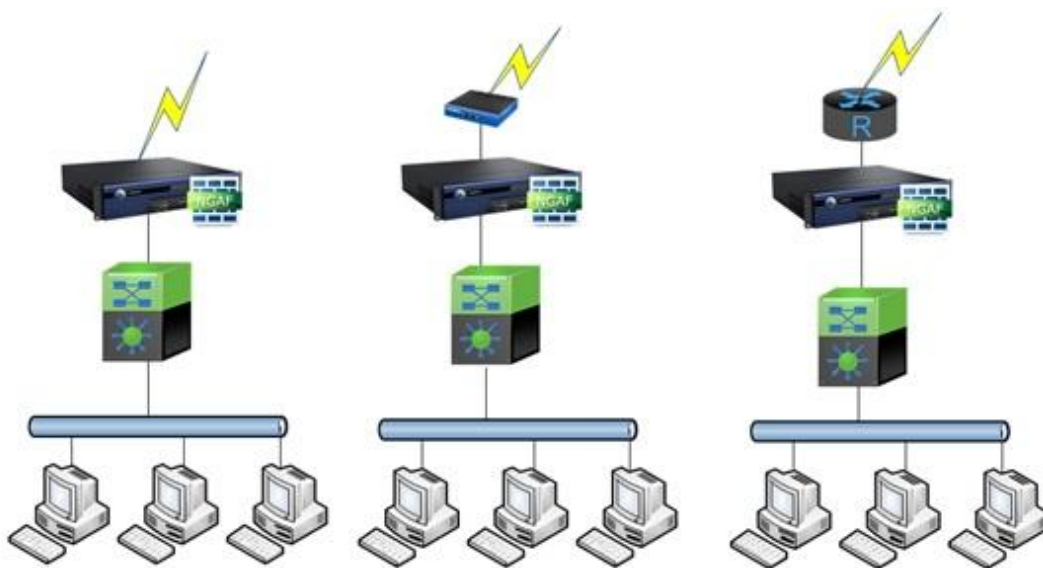
Logs are deleted by day. Logs cannot be deleted individually.

Configuration Examples

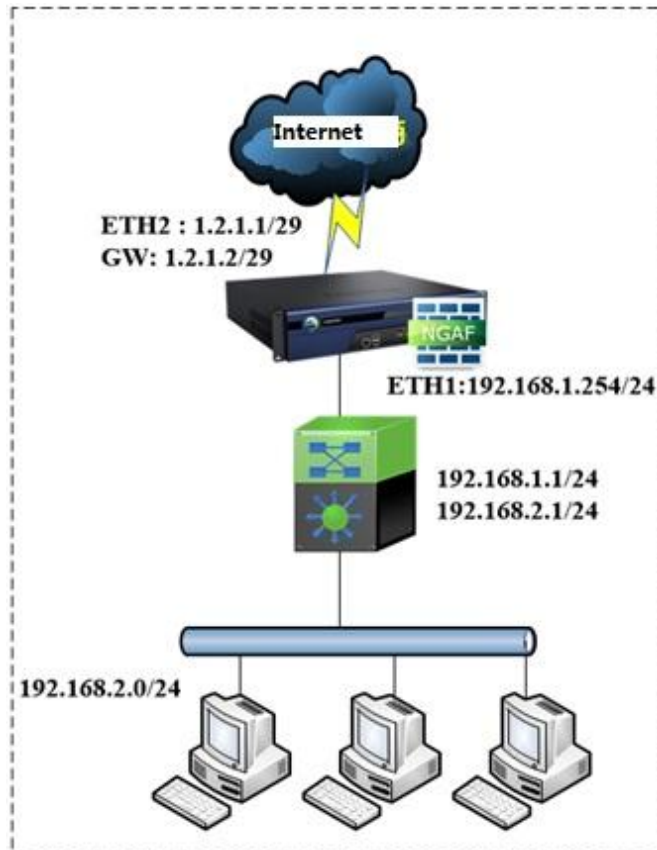
Deployment and Configuration

Router Interface Configuration

In a typical application scenario of router interfaces, the NGAF is deployed at a public network egress as a router and serves as a proxy to enable intranet users to access the Internet.



Configuration example: The following figure shows a network consisting of three layers. The NGAF is deployed at a public network egress and serves as a proxy to enable intranet users to access the Internet. An optical line is used to connect to a public network and assigned with a fixed IP address.



Step 1: Log in to the NGAF by using the default IP address of the management interface (ETH0), which is 10.251.251.251/24. Configure an IP address that is in the same network segment as the default IP address on your PC and log in to the NGAF by using <https://10.251.251.251>.

Step 2: Choose **Network** > **Interface** and click the interface (such as ETH2) to be configured as an Ethernet interface. The following dialog box is displayed.

Edit Physical Interface

☒ Enable

Name: eth2

Description:

Type: Route(layer 3) ▼

Added To Zone: Select zone ▼

Basic Attributes: ☒ WAN attribute ☐ Pingable

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 1.2.1.1/29 ⓘ

Next-Hop IP: 1.2.1.2 ⓘ

Line Bandwidth

Outbound: 10 Mbps ▼

Inbound: 10 Mbps ▼

Link State Detection

A feature that achieves automatic link failover when one of the lines becomes down. [Settings](#)

OK Cancel

Set **Type** to **Route**.


Set **Basic Attributes** to **WAN attribute** if the interface is connected to an uplink, or set it to **Pingable**.

Set **Added To Zone** to the zone which interface ETH2 belongs to (which is a WAN in this example). Set the zone in advance based on section 3.2.1.4.

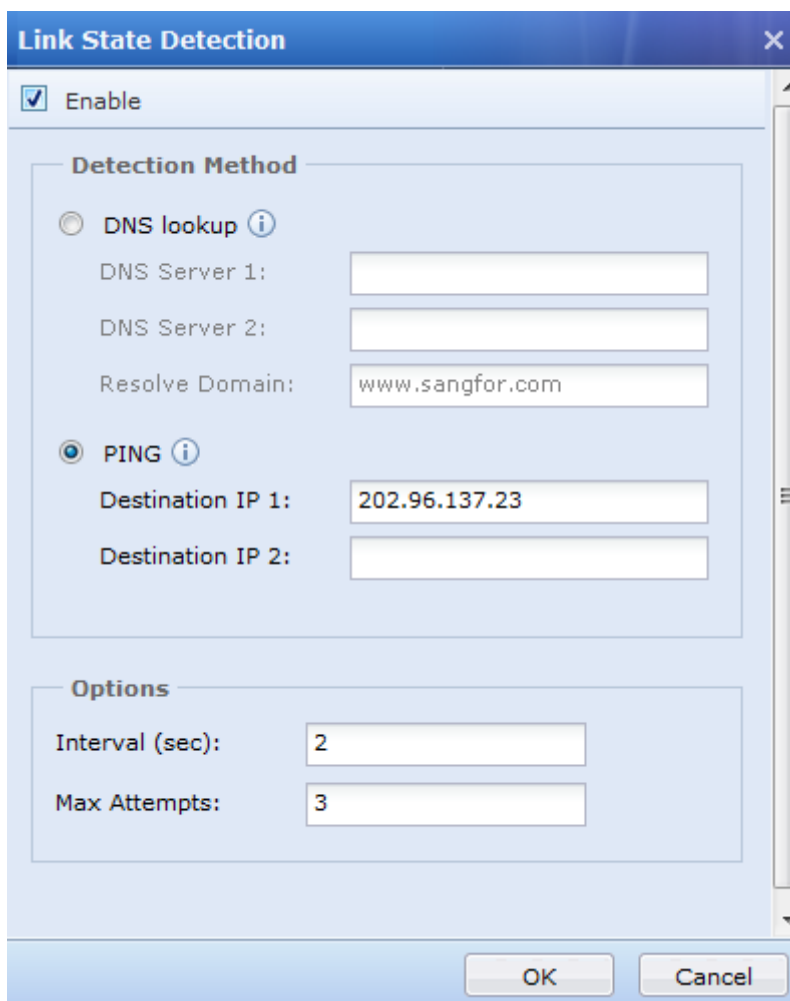
Set **IP Assignment** to **Static**, **DHCP**, or **PPPoE** based on the characteristics of the specified line. If **IP Assignment** is set to **Static**, you need to set **Static IP** and **Next-Hop IP**. If the IP address of the interface is obtained automatically through DHCP, set **IP Assignment** to **DHCP**. If the line uses ADSL dial-up, set the user name, password, and other dial-up parameters.

Static IP can be in the formats of *IP address/mask* and *IP address/mask-HA*. The latter format indicates that the IP address is not synchronized along with the network interface. The format is applicable in the scenario where the NGAF works in hot standby mode.

Set **IP Assignment** to **Static** because the Ethernet interface is connected to an optical line assigned with a static IP address, and configure the public IP address and next-hop gateway assigned to the optical line by an ISP.

Set the uplink and downlink bandwidths of the public link in the **Line Bandwidth** area. Click  to change the bandwidth unit, which is KB/s, MB/s, or GB/s.

Link State Detection enables users to detect link availability. To enable link failure detection, click **Settings**. The **Link State Detection** dialog box is displayed, where you can configure a detection method.



The image shows a 'Link State Detection' dialog box with a blue title bar and a close button. It contains three main sections: 'Enable', 'Detection Method', and 'Options'. The 'Enable' section has a checked checkbox. The 'Detection Method' section has two radio buttons: 'DNS lookup' (unselected) and 'PING' (selected). Below 'DNS lookup' are fields for 'DNS Server 1', 'DNS Server 2', and 'Resolve Domain' (containing 'www.sangfor.com'). Below 'PING' are fields for 'Destination IP 1' (containing '202.96.137.23') and 'Destination IP 2'. The 'Options' section has fields for 'Interval (sec):' (containing '2') and 'Max Attempts:' (containing '3'). At the bottom are 'OK' and 'Cancel' buttons.

Section	Field	Value
Enable	Enable	<input checked="" type="checkbox"/>
	Detection Method	
Detection Method	DNS lookup	<input type="radio"/>
	DNS Server 1	
	DNS Server 2	
	Resolve Domain	www.sangfor.com
	PING	<input checked="" type="radio"/>
Detection Method	Destination IP 1	202.96.137.23
	Destination IP 2	
Options	Interval (sec):	2
	Max Attempts:	3

Select **Enable** to enable link failure detection.

Set **Detection Method** to **DNS lookup** or **PING**. If it is set to **DNS lookup**, set **DNS Server 1**, **DNS Server 2**, and **Resolve Domain**. If it is set to **PING**, set **Destination IP 1** and **Destination IP 2**. Either **DNS lookup** or **PING** can be selected for the same interface. Set **Detection Method** to **PING** and **Destination IP 1** to **202.96.137.23**.

The **Advanced** option enables users to set the operating mode, MTU, and MAC address of the network interface. To modify the settings, click **Settings**.

The screenshot shows a window titled "Advanced" with a close button (X) in the top right corner. Inside the window, there are three configuration fields: "Link Mode:" with a dropdown menu showing "Auto-negotiation", "MTU:" with a text box containing "1500", and "MAC:" with a text box containing "00:E0:4C:46:FA:6E". At the bottom of the window, there are three buttons: "Restore Default MAC", "OK", and "Cancel".



- The next-hop gateway of the interface is only used for link failure detection and PBR of the interface. When a next-hop gateway is configured, the default route 0.0.0.0/0 is not generated on the NGAF. The default route must be configured manually.
- The line bandwidth configuration of the interface is not related to the bandwidth configuration of traffic management. The former is used for PBR scheduling. For more information about PBR, see section 3.2.2.2.

Step 3: Configure an intranet interface. Select an idle network interface and click the interface name to access the **Edit Physical Interface** dialog box. Set **Type** to **Route**, unselect **WAN attribute**, and configure an IP address.

Edit Physical Interface

☒ Enable

Name: eth1

Description:

Type: Route(layer 3) ▼

Added To Zone: WAN ▼

Basic Attributes: ☐ WAN attribute ☐ Pingable

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 192.168.1.254/24 ⓘ

Next-Hop IP: ⓘ

Line Bandwidth

Outbound: 12.5 Mbps ▼

Inbound: 12.5 Mbps ▼

Link State Detection

A feature that achieves automatic link failover when one of the lines becomes down. [Settings](#)

OK Cancel

Step 4: Configure a default route destined to 0.0.0.0/0.0.0.0 that points to the front-end gateway 1.1.1.2. Add the static route destined to various network segments to the layer 3 switch because the intranet interface is connected to multiple network segments through three layers. For static route configuration, see section 3.2.2.1.

Step 5: Configure a proxy to enable intranet users to access the Internet. For details, see section 3.7.1.1.

Step 6: Connect the NGAF to the network. Connect interface ETH2 to the optical line and interface ETH1 to the layer 3 switch on the intranet.



- **When the NGAF works as a router, the gateways of the PCs on the LAN point to the IP address of the intranet interface of the NGAF or the layer 3 switch. The gateway of the layer 3 switch points to the NGAF. Internet access data is provided to NAT on the NGAF or is routed.**

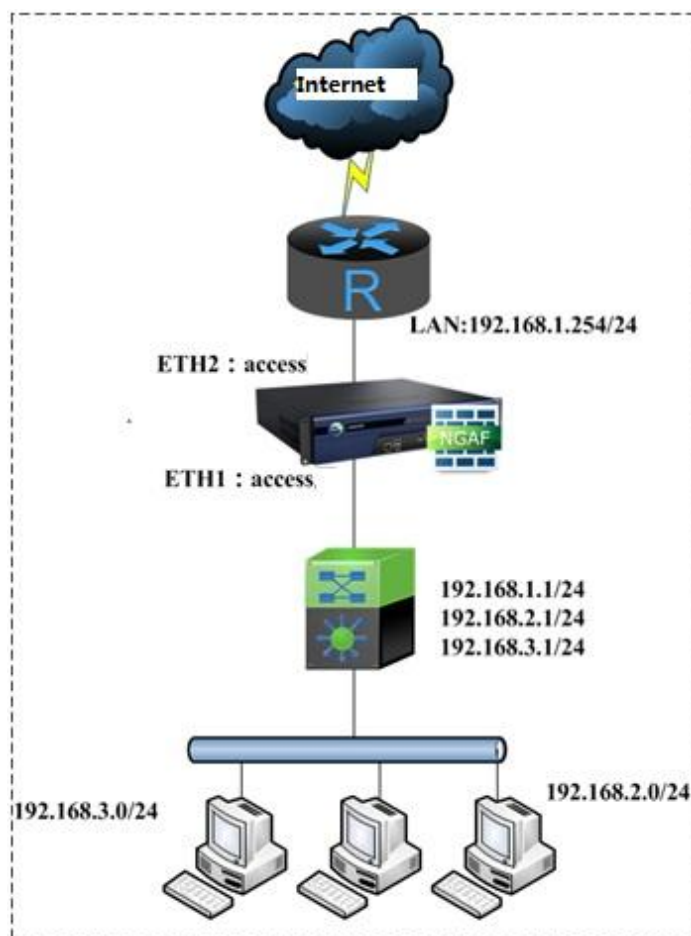
- When the NGAF has multiple router interfaces, they can be configured with IP addresses in the same network segment. The network interface that forwards data is determined by static routing.
- The NGAF allows a router interface configured with multiple WAN attributes to connect to multiple Internet lines, but the interface must be granted with the right of multiline connection.

Transparent Interface Configuration

When the network interface that routes data to or from the NGAF works in transparent mode, the NGAF also works in transparent mode and is considered as a network cable with the filter function. The transparent mode is used when it is difficult to modify the existing network topology. The NGAF is connected between existing gateways and intranet users. The configurations of the gateways and intranet users are not modified, and only basic configurations of the NGAF are required. The main feature of the transparent mode is that the NGAF is invisible to users. Transparent interfaces are classified into access interfaces and trunk interfaces.

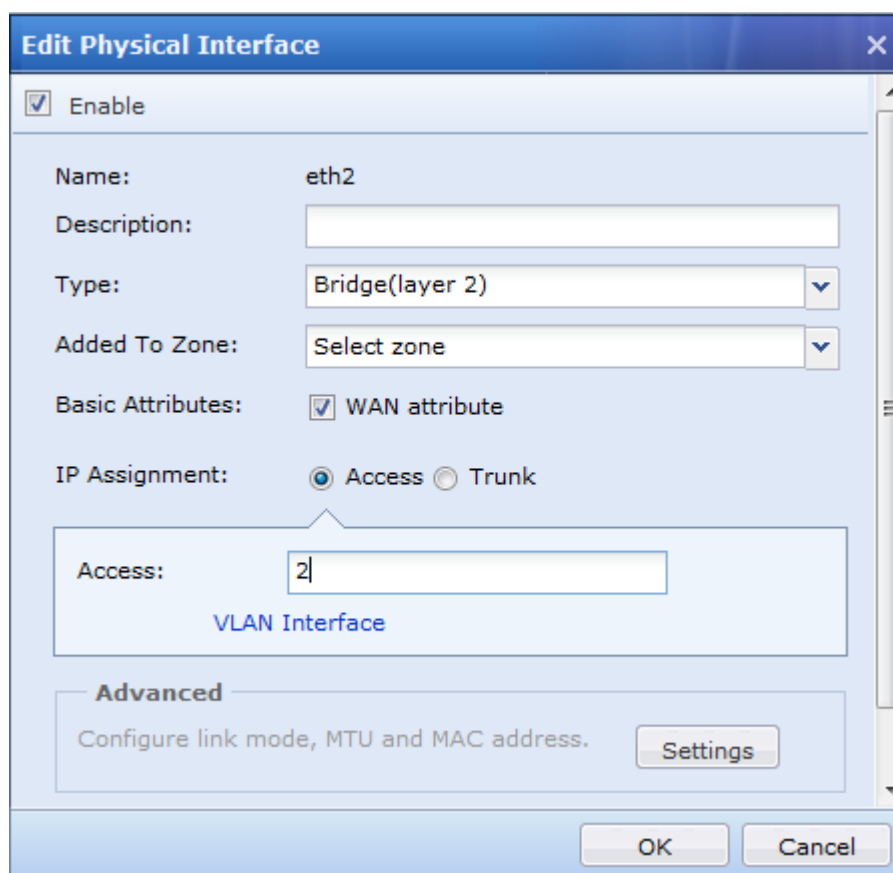
Access Interface Configuration

Configuration example: The following figure shows a network topology where the NGAF works in transparent mode and the intranet is connected to a layer 3 switch and has two network segments: 192.168.2.0/255.255.255.0 and 192.168.3.0/255.255.255.0.



Step 1: Log in to the NGAF by using the default IP address of the management port (ETH0), which is 10.251.251.251/24. Configure an IP address that is in the same network segment as the default IP address on your PC and log in to the NGAF by using https://10.251.251.251.

Step 2: Choose **Network > Interface > Physical Interface** and click the interface (such as ETH2) to be configured as an Ethernet interface. The following dialog box is displayed.



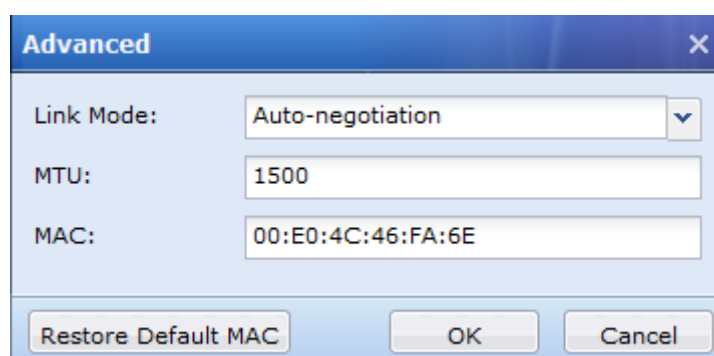
Set Type to Transparent.

Set Added To Zone to the zone which interface ETH2 belongs to (which is a WAN in this example). Set the zone in advance based on section 3.2.1.4.

Set Basic Attributes to WAN attribute if the interface connects to an uplink.

Set IP Assignment to Access. The access interface is the VLAN1 interface and does not need to be changed, but it can be set to another VLAN interface. The two interfaces of the NGAF must be on the same VLAN.

The Advanced option enables users to set the operating mode, MTU, and MAC address of the network interface. To modify the settings, click Settings.



Step 3: Configure an intranet interface. Select an idle network interface and click the interface name to access the **Edit Physical Interface** dialog box. Set **Type** to **Transparent**, unselect **WAN attribute**, and set **IP Assignment** to **Access**.

Edit Physical Interface

☒ Enable

Name: eth1

Description:

Type: Bridge(layer 2) ▼

Added To Zone: LAN ▼

Basic Attributes: ☐ WAN attribute

IP Assignment: ☒ Access ☐ Trunk

Access: 2

VLAN Interface

Advanced

Configure link mode, MTU and MAC address. Settings

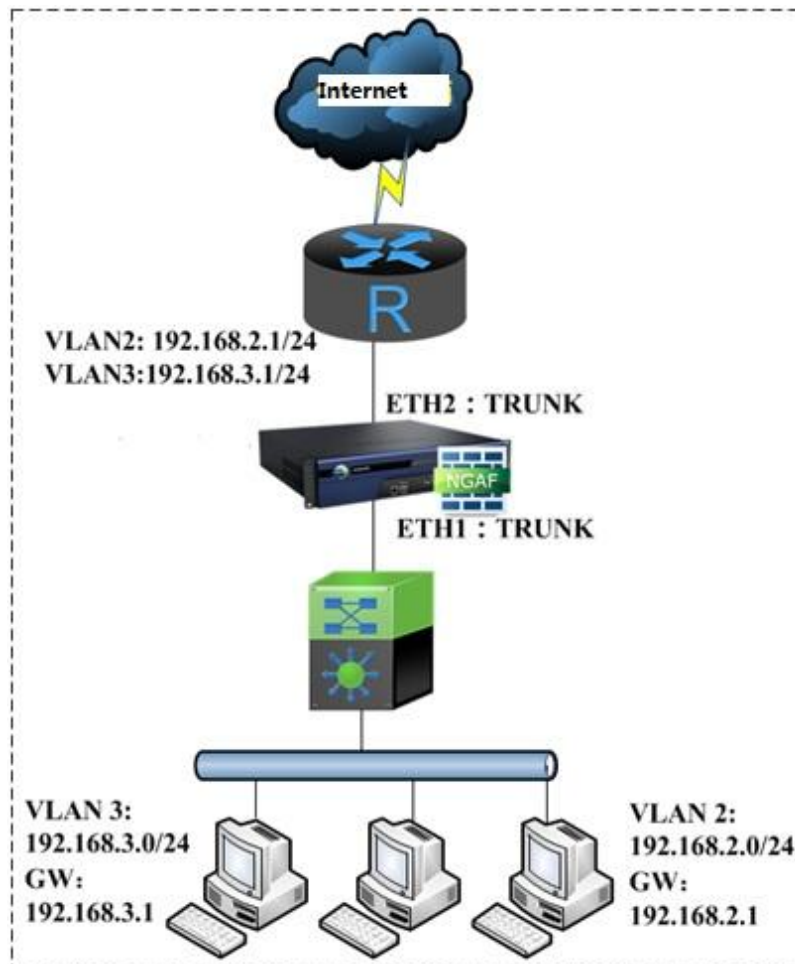
OK Cancel

Step 4: Configure a VLAN interface and set the corresponding IP address. The IP address can be used to log in to the console of the NGAF for management. For details about how to configure a VLAN interface, see section 3.2.1.3. A special management interface can also be used to log in to the NGAF.

Step 5: Connect the NGAF to the network. Connect interface ETH2 to the front-end router and interface ETH1 to the layer 3 switch on the intranet.

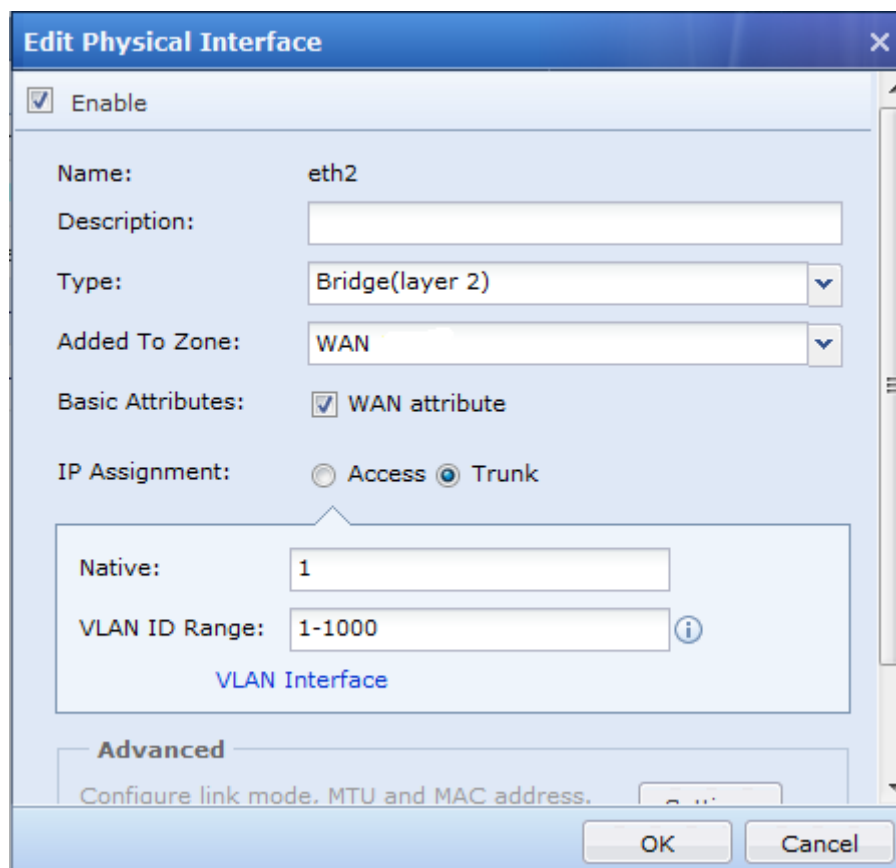
Trunk Interface Configuration

Configuration example: The following figure shows a network topology where the NGAF works in transparent mode, the switch on the intranet is divided into VLANs but does not enable routing, and the front-end router works as a gateway for various VLANs. The intranet has two network segments: 192.168.2.0/255.255.255.0 and 192.168.3.0/255.255.255.0, which belong to VLAN2 and VLAN3 respectively. A trunk protocol is used between the switch and router.



Step 1: Log in to the NGAF by using the default IP address of the management port (ETH0), which is 10.251.251.251/24. Configure an IP address that is in the same network segment as the default IP address on your PC and log in to the NGAF by using <https://10.251.251.251>.

Step 2: Choose **Network** > **Interface** and click the interface (such as ETH2) to be configured as an Ethernet interface. The following dialog box is displayed.



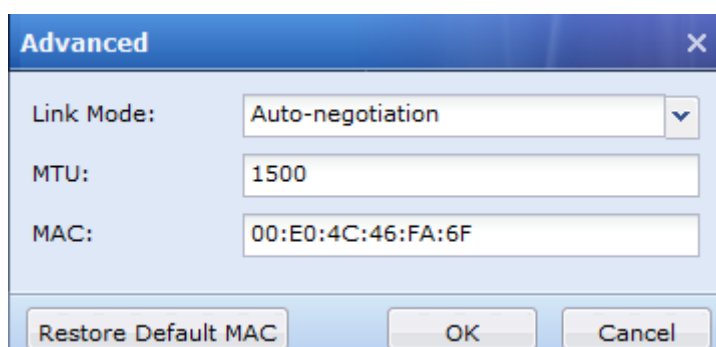
Set **Type** to Transparent.

Set **Added To Zone** to the zone which interface ETH2 belongs to (which is a WAN in this example). Set the zone in advance based on section 3.2.1.4.

Set **Basic Attributes** to WAN attribute if the interface connects to an uplink.

Set **IP Assignment** to Trunk. The values of the Native (set to 1 by default) and VLAN ID Range (set to 1-1000 by default) fields do not need to be changed. VLAN ID Range can also be set to the VLAN IDs that will go through device; so set VLAN ID Range to 2-3.

The Advanced option enables users to set the operating mode, MTU, and MAC address of the network interface. To modify the settings, click Settings.



Step 3: Configure an intranet interface. Select an idle network interface and click the interface name to access the **Edit Physical Interface** dialog box. Set **Type** to Transparent, unselect **WAN attribute**, and set **IP Assignment** to **Trunk**.

Edit Physical Interface

☒ Enable

Name: eth1

Description:

Type: Bridge(layer 2) ▼

Added To Zone: LAN ▼

Basic Attributes: ☐ WAN attribute

IP Assignment: ☐ Access ☒ Trunk

Native: 1

VLAN ID Range: 1-1000 ⓘ

VLAN Interface

Advanced

Configure link mode, MTU and MAC address.

Step 4: Configure VLAN2 and VLAN3 interfaces in the **Add VLAN Interface** dialog box.

Add VLAN Interface

Name:

Veth.2

Description:

Added To Zone:

Select zone

Basic Attributes:

☒ Pingable

IP Assignment:

☒ Static☐ DHCP

Static IP:

Type here

Next-Hop IP:

Link State Detection

A feature that achieves automatic link failover when one of the lines becomes down.

Settings

Advanced

Specify Maximum Transmission Unit (MTU).

Settings

OK

Cancel

Add VLAN Interface

Name: Veth. 3 ⓘ

Description:

Added To Zone: Select zone ▼

Basic Attributes: ☒ Pingable

IP Assignment: ☒ Static ☐ DHCP

Static IP: ⓘ

Next-Hop IP:

Link State Detection

A feature that achieves automatic link failover when one of the lines becomes down. [Settings](#)

Advanced

Specify Maximum Transmission Unit (MTU). [Settings](#)

OK Cancel

Interfaces								
Physical Interface Sub-Interface VLAN Interface Aggregate Interface Zone Link State Propagation								
+ Add - Delete Refresh								
<input type="checkbox"/> Name	Zone	IP Assignment	IP Address	MTU	Ping	Link State	Delete	
<input type="checkbox"/>								
<input type="checkbox"/> veth.3	None ⓘ	Static	---	1500	Allow	Not detected yet	✗	
<input type="checkbox"/> veth.2	None ⓘ	Static	---	1500	Allow	Not detected yet	✗	

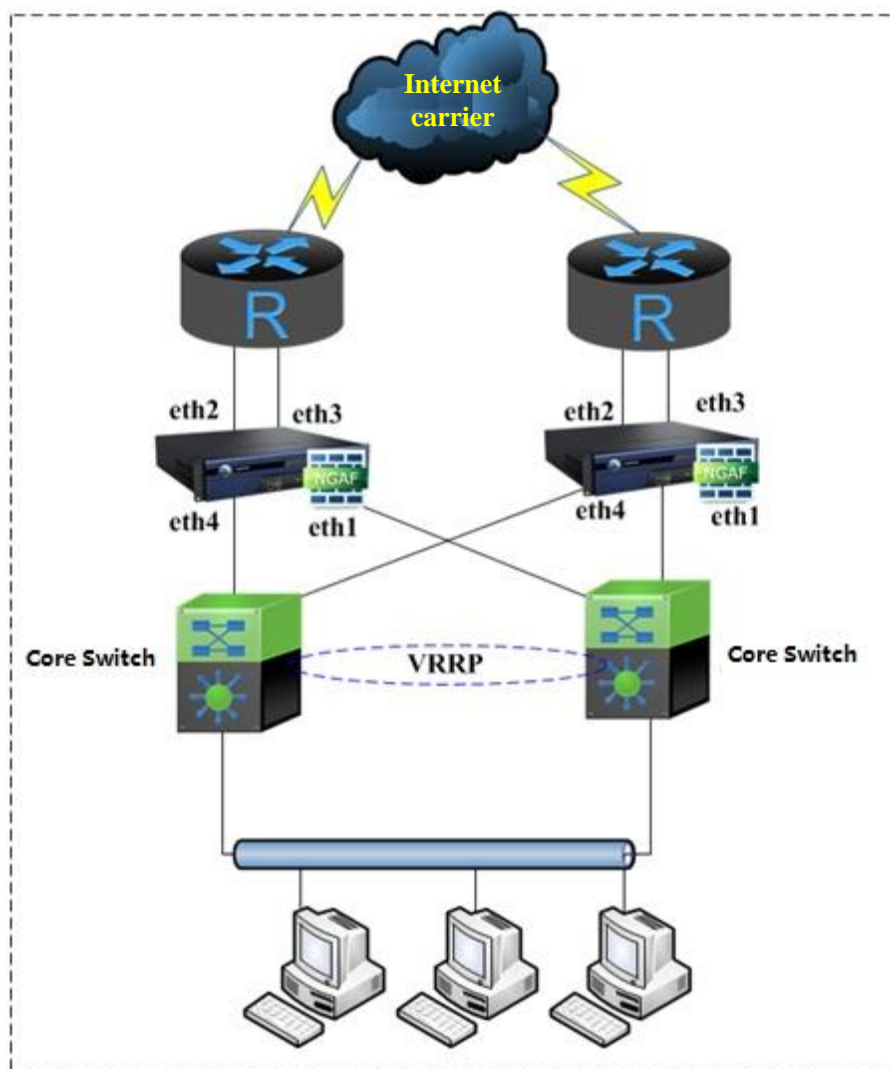
Step 5: Connect the NGAF to the network. Connect interface ETH2 to the front-end router and interface ETH1 to the layer 3 switch on the intranet.



- In the network environment described above, virtual wire interfaces can be deployed and virtual wires are recommended. For configuration details, see section 2.1.3.
- The IP addresses and gateways of the VLAN interfaces can be left unspecified.

Virtual Wire Interface Configuration

Configuration example: The following figure shows a network environment where two layer 3 switches and two routers are deployed on the intranet for load balancing and The NGAF is deployed in transparent mode, not changing the original Internet access mode.



To deploy the NGAF in transparent mode, layer 2 isolation must be configured between the ETH4 and ETH2 pair and the ETH1 and ETH3 pair. Data flowing to interface ETH4 must be forwarded through interface ETH2, and data flowing to interface ETH1 must be forwarded through interface ETH3. This can be realized by configuring virtual wire interfaces.

Step 1: Log in to the NGAF by using the default IP address of the management port (ETH0), which is 10.251.251.251/24. Configure an IP address that is in the same network segment as the default IP address on your PC and log in to the NGAF by using <https://10.251.251.251>.

Step 2: Choose **Network > Interface** and click the interface (such as ETH2) to be configured as an Ethernet interface. The following dialog box is displayed.

Edit Physical Interface

☒ Enable

Name: eth2

Description: external

Type: Virtual wire(layer 1) ▼

Added To Zone: Select zone ▼

Interface 1: eth2

Interface 2: eth1 ▼

Basic Attributes: ☒ WAN attribute

Advanced

Configure link mode, MTU and MAC address. Settings

OK Cancel

Set Type to Virtual wire.

The Virtual Wire page is displayed, providing the option of setting interface pairs of the virtual wire. For details, see section 3.2.3.

Set Added To Zone to the zone which interface ETH2 belongs to (which is a WAN in this example). Set the zone in advance based on section 3.2.1.4.

Set Basic Attributes to WAN attribute if the interface connects to an uplink.

The Advanced option enables users to set the operating mode, MTU, and MAC address of the network interface. To modify the settings, click Settings.

Advanced

Link Mode: Auto-negotiation ▼

MTU: 1500

MAC: 00:0B:AB:55:DC:1D

Restore Default MAC OK Cancel

Click **OK**. Use the same method to set the Ethernet interface ETH3.

Step 3: Configure an intranet interface. Select an idle network interface and click the interface name to access the **Edit Physical Interface** dialog box. Set **Type** to **Virtual wire** and unselect **WAN attribute**.

Click **OK**. Use the same method to set the intranet interface ETH4.

Step 4: Set a virtual wire. Choose **Network > Interface > Virtual Wire** to add a virtual wire. For details, see section 3.2.3.

Step 5: Configure switchover for the switches and routers on the intranet. Choose **Network > Interface > Link State Propagation** and enable interface propagation. For details, see section 3.2.1.6.

Step 6: Connect the NGAF to the network. Connect interfaces ETH2 and ETH3 to the front-end routers and interfaces ETH4 and ETH1 to the layer 3 switches on the intranet.

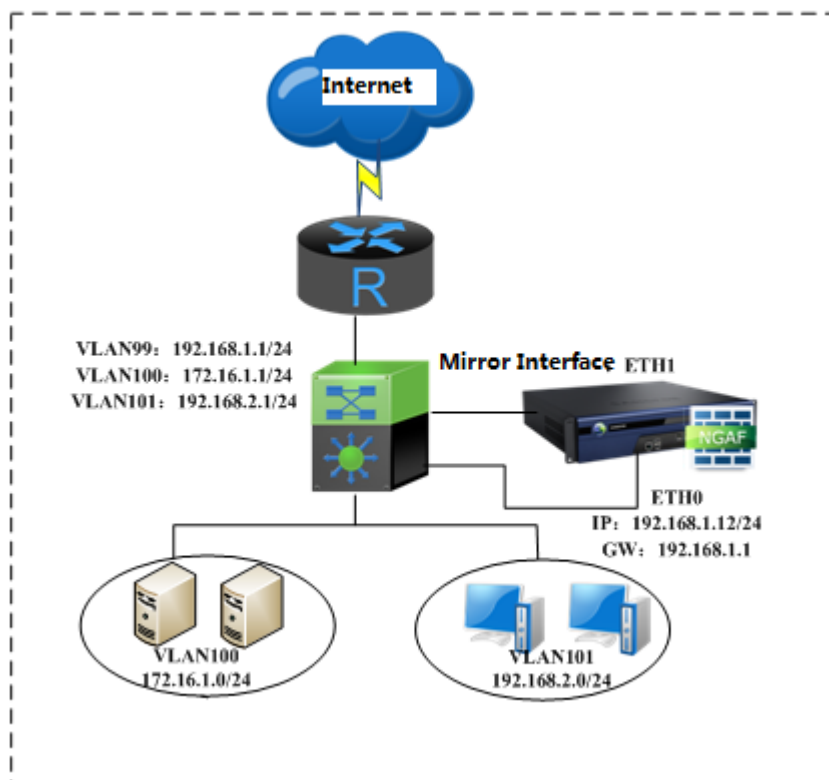


The management interface cannot be configured as a virtual wire interface. If two or more pairs of virtual wires must be configured, the NGAF needs to have at least five interfaces. Except for an interface that must be configured as the management interface, the remaining interfaces can be configured as virtual wire interfaces.

Bypass Mirror Interface Configuration

Bypass mode: A network environment does not need to be modified to implement protection. The risk of network interruption caused by device malfunction can be avoided. The NGAF is connected to the mirror interface of a switch or to a hub so that an Internet user accesses the data of a server through the switch or hub. Upstream and downstream data must be mirrored when the mirror interface is configured to realize server protection.

Configuration example: The following figure shows the network topology where the NGAF is deployed in bypass mode, the user network segment is 192.168.2.0/24, and the server network segment is 172.16.1.0/24. The NGAF is required to implement IPS protection and web application protection and prevent sensitive data leak on servers.



Step 1: Log in to the NGAF by using the default IP address of the management port (ETH0), which is 10.251.251.251/24. Configure an IP address that is in the same network segment as the default IP address on your PC and log in to the NGAF by using <https://10.251.251.251>.

Step 2: Configure a management interface. When the NGAF is deployed in bypass mode, it blocks connections through the management interface. Choose **Network > Interface > Physical Interface** and click **eth0**. The **Edit Physical Interface** dialog box is displayed.

Edit Physical Interface

☒ Enable

Name: eth0

Description: Manage interface

Type: Route(layer 3) ▼

Added To Zone: Select zone ▼

Basic Attributes: ☒ WAN attribute ☒ Pingable

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 10.251.251.251/24
192.168.1.12/24 ⓘ

Next-Hop IP: 192.168.1.1 ⓘ

Line Bandwidth

Outbound: 1024 Mbps ▼

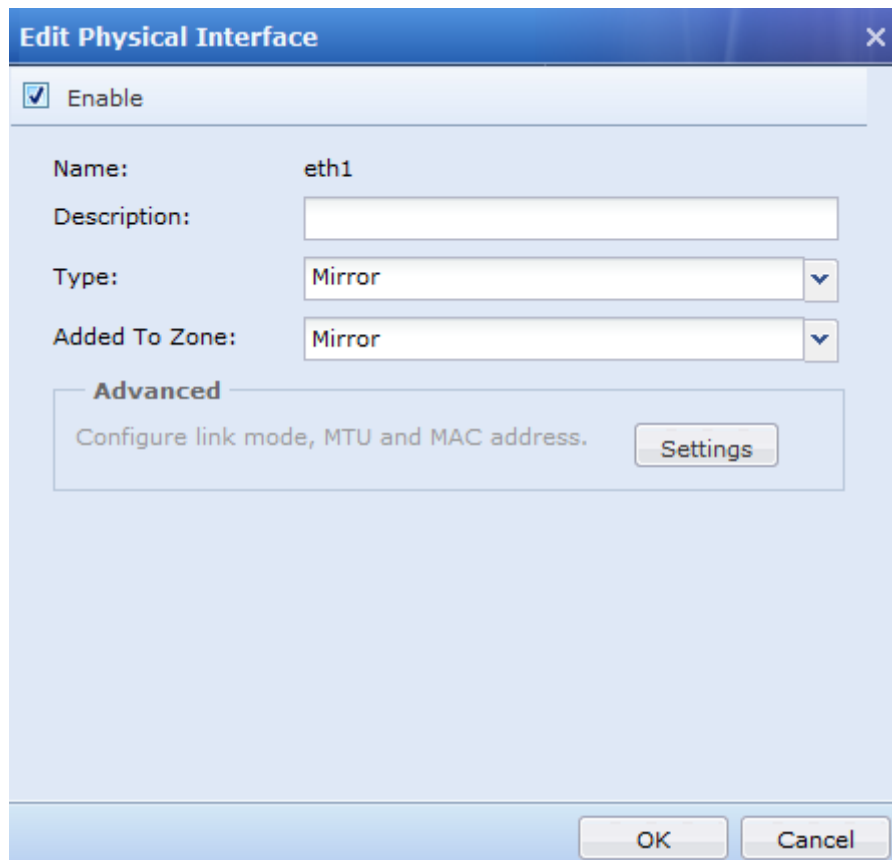
Inbound: 1024 Mbps ▼

Link State Detection

A feature that achieves automatic link failover when one of the lines becomes down. [Settings](#)

OK Cancel

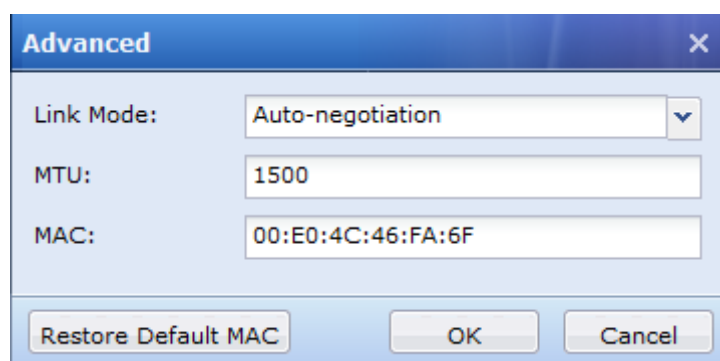
Step 3: Configure a bypass mirror interface. Choose **Network > Interface > Physical Interface** and click **eth1**. The **Edit Physical Interface** dialog box is displayed.



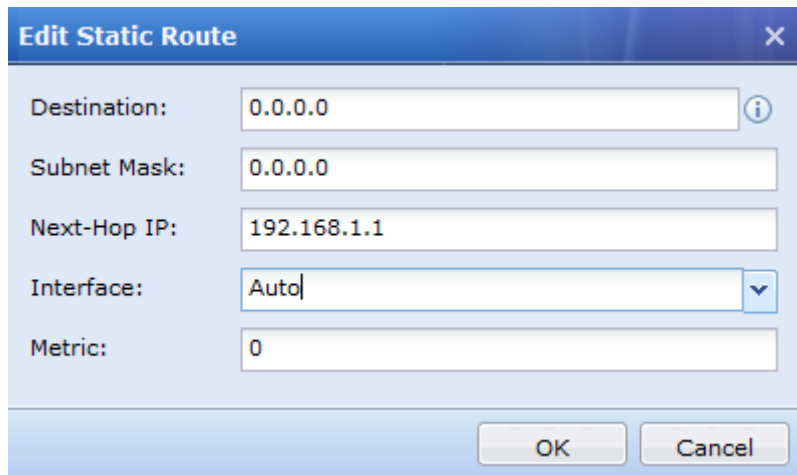
Set Type to Mirror.

Set Added To Zone to the zone which interface ETH1 belongs to (which is a mirror zone in this example). Set the zone in advance based on section 3.2.1.4.

The Advanced option enables users to set the operating mode, MTU, and MAC address of the network interface. To modify the settings, click Settings.



Step 4: Configure a default route destined to 0.0.0.0/0.0.0 that points to the front-end gateway 192.168.1.1. Choose **Network > Routing > Static Route**. The **Edit Static Route** dialog box is displayed.



Edit Static Route

Destination: 0.0.0.0

Subnet Mask: 0.0.0.0

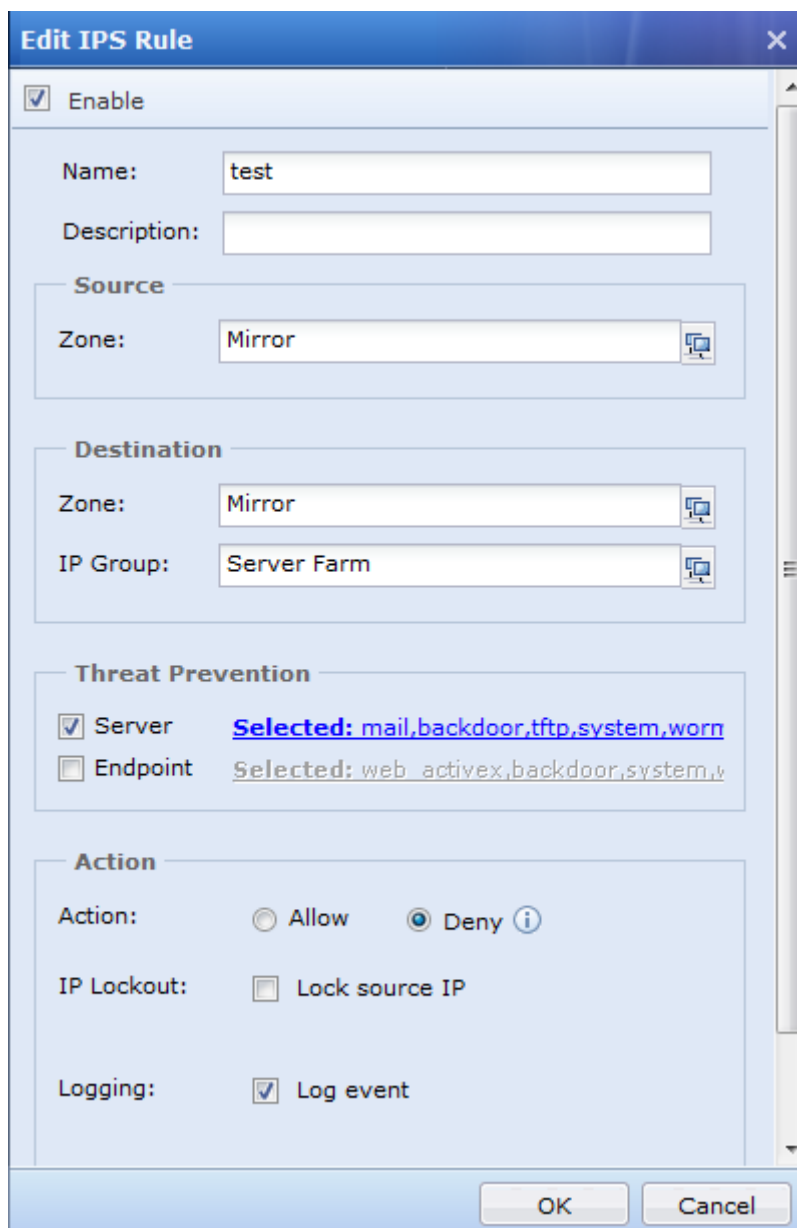
Next-Hop IP: 192.168.1.1

Interface: Auto

Metric: 0

OK Cancel

Step 5: Configure a protection rule. Choose **IPS > IPS** to configure an IPS rule in bypass mode. The **Edit IPS Rule** dialog box is displayed.



Edit IPS Rule

☒ Enable

Name: test

Description:

Source

Zone: Mirror

Destination

Zone: Mirror

IP Group: Server Farm

Threat Prevention

☒ Server [Selected: mail,backdoor,tftp,system,worm](#)

☐ Endpoint [Selected: web_activex,backdoor,system,w](#)

Action

Action: ☐ Allow ☒ Deny

IP Lockout: ☐ Lock source IP

Logging: ☒ Log event

OK Cancel

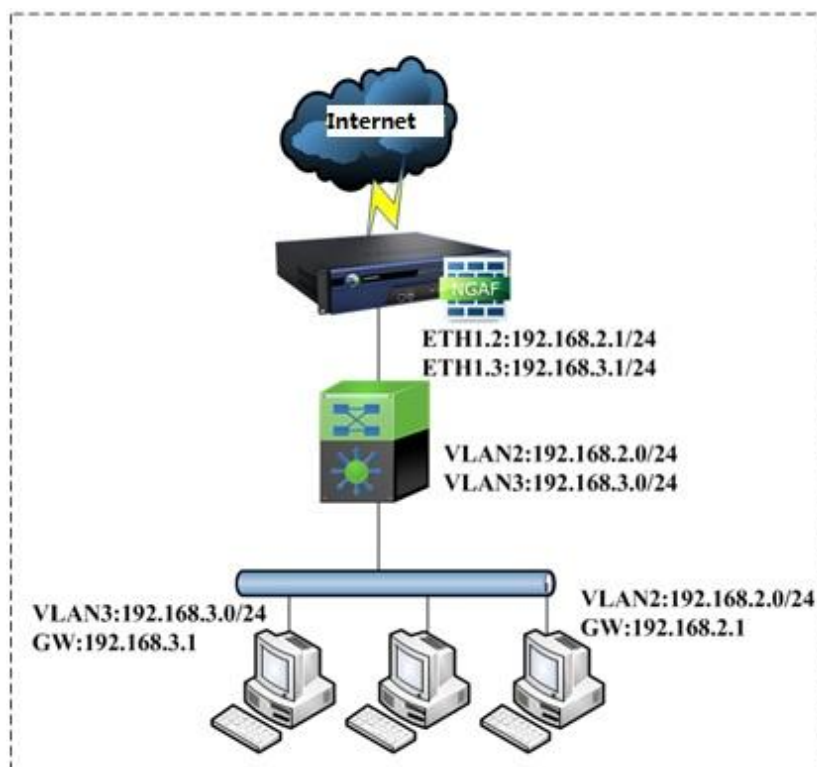
In bypass mode, set the source and destination zones to the zone which the bypass mirror interface belongs to, and

set the destination IP address group to the IP address group which the server network segment belongs to.

Step 6: Connect the NGAF to the network, interface ETH1 to the bypass mirror interface of the layer 3 switch, and interface ETH0 to an interface of VLAN99 of the layer 3 switch on the intranet.

Subinterface Configuration

Configuration example: The following figure shows the network environment where the switch on the intranet is divided into two VLANs, intranet users are grouped to VLAN2 and VLAN3, and the NGAF provides the routing function between the VLANs and works as a gateway for the VLANs on the intranet.



Step 1: Choose **Network > Interface > Physical Interface** and click the interface (such as ETH2) to be configured as an intranet interface. Configure the intranet interface as a router interface, unselect **WAN attribute**, and set the IP address and gateway of the intranet interface based on requirements.

Edit Physical Interface

☒ Enable

Name: eth2

Description:

Type: Route(layer 3) ▼

Added To Zone: Select zone ▼

Basic Attributes: ☐ WAN attribute ☐ Pingable

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 1.1.1.3/29 ⓘ

Next-Hop IP: ⓘ

Line Bandwidth

Outbound: 1024 Mbps ▼

Inbound: 1024 Mbps ▼

Link State Detection

A feature that achieves automatic link failover when one of the lines becomes down. [Settings](#)

OK Cancel

Step 2: Add a VLAN subinterface. Choose **Network > Interface > Sub-Interface** and click **Add**. The **Add Sub-Interface** dialog box is displayed.

Physical Interface: specifies the physical interface to which the subinterface is added. Only a router interface can be added with a subinterface.

VLAN ID: specifies the VLAN ID of the subinterface.

IP Assignment: can be set to **Static** or **DHCP**. If it is set to **Static**, fill in the **Static IP** field with the gateway address of the corresponding VLAN.

The setting of **Link State Detection** and **Advanced** is the same as that of a router interface.

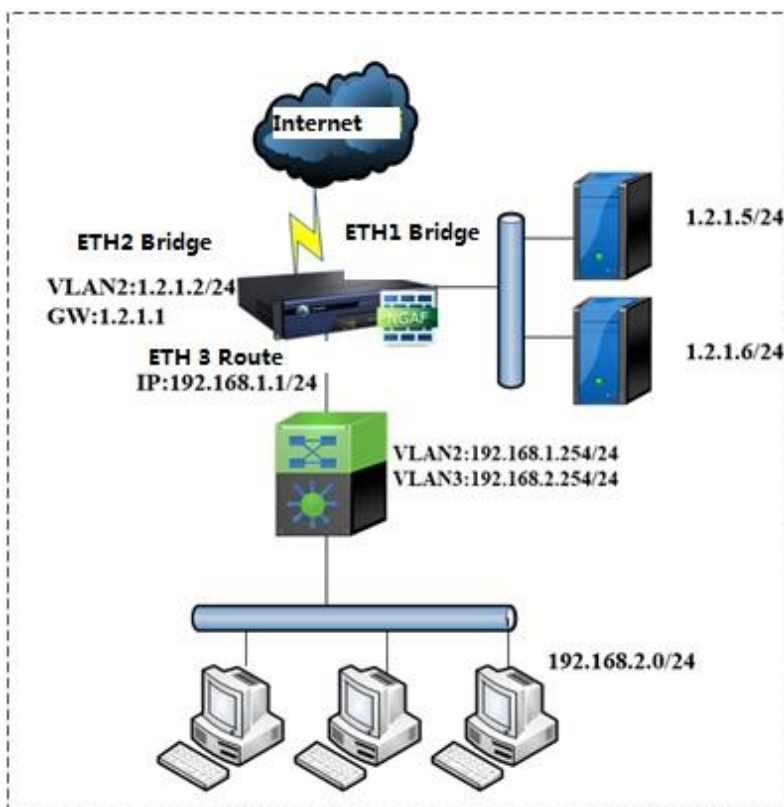
Click **OK**. Repeat the preceding steps to add a subinterface to VLAN3.



A physical interface can be added with multiple subinterfaces. The IP address of the physical interface must be in a different network segment from that of any of its subinterfaces.

Hybrid Deployment

Configuration example: The following figure shows a network topology where the intranet has a massive server cluster, which must be accessed by users through a public network. Each server is assigned a public IP address. The NGAF is deployed at a public network egress to enable users to access the server cluster by using public IP addresses. Servers cannot be advertised through port mapping. The NGAF can serve as a proxy to enable intranet users to access the Internet.



To enable users to access servers by using the corresponding public IP addresses, configure EHT2 of the NGAF connecting to a public network and EHT1 of the NGAF connecting to the server cluster on the LAN as transparent access interfaces on the same VLAN. Configure a VLAN interface and the corresponding public IP address. Configure interface ETH3 connecting to the intranet as a router interface. When an intranet user accesses a public network, the source IP address is converted to the public IP address of the VLAN interface.

Step 1: Configure the Ethernet interface ETH2. Choose **Network > Interface > Physical Interface** and click **eth2**. The **Edit Physical Interface** dialog box is displayed. Perform configuration as shown in the following figure.

Edit Physical Interface

☒ Enable

Name: eth2

Description:

Type: Bridge(layer 2) ▼

Added To Zone: LAN ▼

Basic Attributes: ☒ WAN attribute

IP Assignment: ☒ Access ☐ Trunk

Access: 2
VLAN Interface

Advanced

Configure link mode, MTU and MAC address. Settings

OK Cancel

Step 1: Configure the intranet interface ETH1. Choose **Network > Interface > Physical Interface** and click **eth1**. The **Edit Physical Interface** dialog box is displayed. Perform configuration as shown in the following figure.

Edit Physical Interface

☒ Enable

Name: eth1

Description:

Type: Bridge(layer 2) ▼

Added To Zone: Select zone ▼

Basic Attributes: ☒ WAN attribute

IP Assignment: ☒ Access ☐ Trunk

Access: 2
VLAN Interface

Advanced

Configure link mode, MTU and MAC address. Settings

OK Cancel

Step 1: Configure the intranet interface ETH3. Choose **Network > Interface > Physical Interface** and click **eth3**.

The **Edit Physical Interface** dialog box is displayed. Perform configuration as shown in the following figure.

Edit Physical Interface

☒ Enable

Name: eth3

Description:

Type: Route(layer 3) ▼

Added To Zone: Select zone ▼

Basic Attributes: ☐ WAN attribute ☐ Pingable

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 192.168.1.1/24 ⓘ

Next-Hop IP: 192.168.1.254 ⓘ

Line Bandwidth

Outbound: 1024 Mbps ▼

Inbound: 1024 Mbps ▼

Link State Detection

A feature that achieves automatic link failover when one of the lines becomes down. [Settings](#)

OK Cancel

Step 4: Configure a VLAN interface. Choose **Network > Interface > VLAN Interface** and click **Add**. The **Edit VLAN Interface** dialog box is displayed. Perform configuration as shown in the following figure.

Edit VLAN Interface

Name: Veth.2

Description:

Added To Zone: Select zone

Basic Attributes: ☒ Pingable

IP Assignment: ☒ Static ☐ DHCP

Static IP: 1.2.1.2/24

Next-Hop IP:

Link State Detection

A feature that achieves automatic link failover when one of the lines becomes down.

Settings

OK Cancel

Step 5: Choose **Network > Routing > Static Route**. Configure the default route of Internet access and the packet reception route.

Edit Static Route

Destination: 0.0.0.0

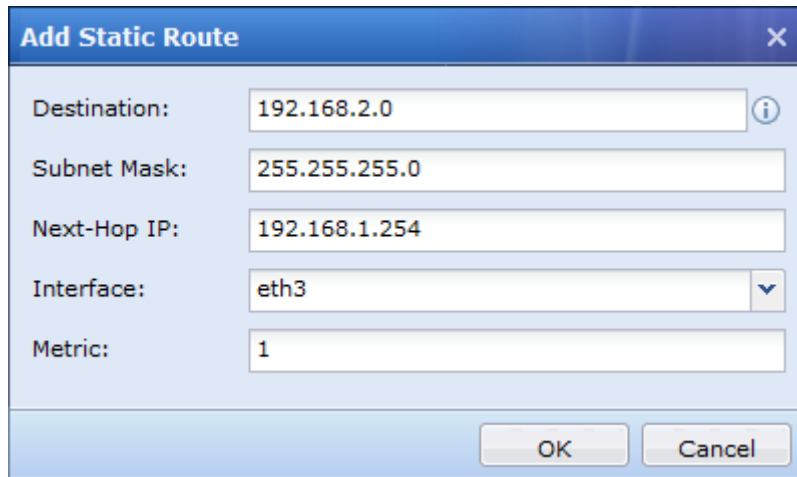
Subnet Mask: 0.0.0.0

Next-Hop IP: 1.2.1.2

Interface: veth.2

Metric: 0

OK Cancel

A screenshot of a 'Add Static Route' dialog box. The dialog has a blue title bar with the text 'Add Static Route' and a close button (X). It contains five input fields: 'Destination:' with the value '192.168.2.0', 'Subnet Mask:' with '255.255.255.0', 'Next-Hop IP:' with '192.168.1.254', 'Interface:' with a dropdown menu showing 'eth3', and 'Metric:' with '1'. At the bottom right are 'OK' and 'Cancel' buttons.

Destination:	192.168.2.0
Subnet Mask:	255.255.255.0
Next-Hop IP:	192.168.1.254
Interface:	eth3
Metric:	1

Configure NAT. For details, see section 3.7.


Policy Based Routing Configuration

Example 1

Configuration example: A user needs to access an e-bank (IP address: 127.8.66.42) over HTTPS. The e-bank checks the connected IP address. When the source IP address of the same connection is changed, the e-bank disconnects, causing an access failure. To solve the problem, configure a PBR so that data destined to the destination IP address is always routed out along the line connected to interface ETH3.


Choose **Network > Routing > Policy-Based Routing** from the navigation menu and click **Add**. The **Add Source-Based Route** dialog box is added.

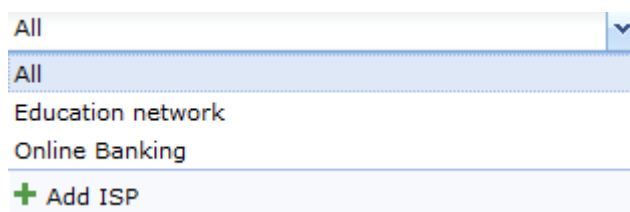
Name and **Description**: specifies the name and description of the PBR.

Schedule: specifies the effective time of the PBR. Click  to select a schedule.

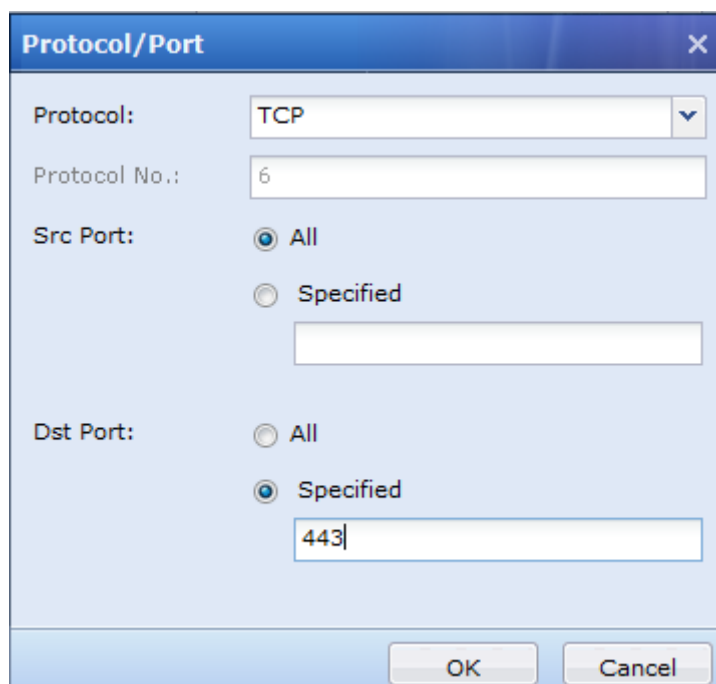
Source: contains the **Zone** (mandatory) and **IP Group** fields.

Destination: contains the **IP Group** and **ISP** options (select one of them). In this example, The HTTPS application

used to access the destination IP address 127.8.66.42 must be matched with the PBR. Click  of the **IP Group** dropdown list to select an option.



Protocol/Port: specifies the protocol and port conditions. Click **Settings**. The **Protocol/Port** dialog box is displayed.



Egress Interface/Next-Hop: specifies the interface or next hop that forwards compliant data packets.

Click **OK**. The new PBR is displayed on the **Policy-Based Routing** page.

Routing														
Static Route			Policy-Based Routing			OSPF			RIP			All Routes		
+ Add - Delete ✓ Enable ✗ Disable ↑ Move Up ↓ Move Down ↻ Move ↺ Refresh 📁 Import 📄 Export														
<input type="checkbox"/>	No.	Name	Source Zone	Src IP Group	Dst IP Group	Protocol	Application	Interface-Next Hop	Load Balanci...	Schedule	Status	Del...		
<input type="checkbox"/>	1	Online bank...	LAN	All 0.0.0.0-255.255.25...	Online Banking	TCP:All->443	All/All	eth3 172.16.1.2		All week	✓	✗		

Example 2

Configuration example: There are two Ethernet lines connected to the Internet, which are 2 Mbit/s and 10 Mbit/s lines of China Telecom. The line with the lightest traffic must be selected automatically for intranet users to access a public network.

Choose **Network > Routing > Policy-Based Routing** from the navigation menu and click **Add**. The **Add Link Load-Balancing Route** dialog box is added.

Add Link Load-Balancing Route

Name:

Description:

Schedule:

Source

Zone:

IP Group:

Destination

IP Group:

ISP:

Protocol/Port

Protocol and port match clauses

Application


Applicable applications

Interface

Interface	Link State	Move	Delete
<input type="checkbox"/> eth2	Not detected yet	↑ ↓	✗
<input type="checkbox"/> eth3	Not detected yet	↑ ↓	✗

Load Balancing Method:

Name and **Description**: specifies the name and description of the PBR.

Schedule: specifies the effective time of the PBR. Click  to select a schedule.

All week

-----Recurring Schedule-----


All week

-----One-Time Schedule-----

+ Add One-Time Schedule

+ Add Recurring Schedule

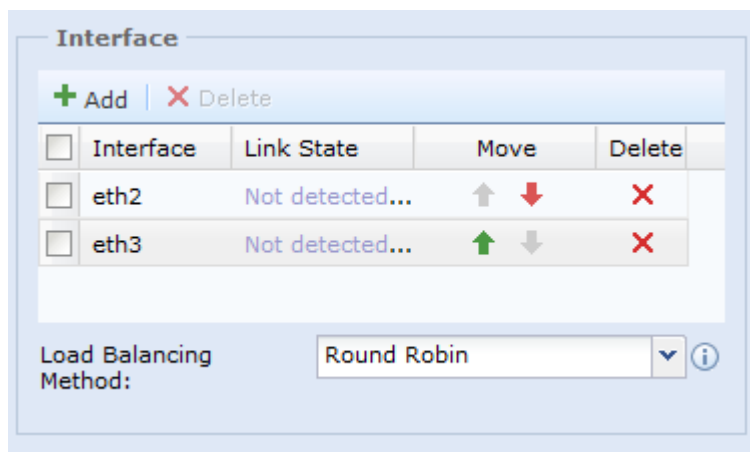
Source: contains the **Zone** (mandatory) and **IP Group** fields.

Destination: contains the **IP Group** and **ISP** options (select one of them). Click  of the **IP Group** dropdown

list to select an option. Before setting an ISP address, set an ISP address database. For details, see section 3.5.1. In this example, all applications used to access a public network must be matched with the PBR; therefore, select all IP addresses.

Protocol/Port: specifies protocol and port conditions. In this example, the PBR is applied to the applications used by all intranet users to access a public network; therefore, **Protocol/Port** does not need to be configured, indicating all protocols and ports.

Interface: specifies the lines for load balancing. Load balancing is implemented for two Ethernet lines. Click **Add** and select the interfaces connected to the two Ethernet lines.



<input type="checkbox"/>	Interface	Link State	Move	Delete
<input type="checkbox"/>	eth2	Not detected...	↑ ↓	×
<input type="checkbox"/>	eth3	Not detected...	↑ ↓	×

Load Balancing Method: Round Robin

Load Balancing Method: specifies a scheduling algorithm for Ethernet lines. Four algorithms are supported, that is, round robin, bandwidth ratio, weight minimum traffic, preferred use of the preceding line.

Round robin: Connections are distributed to multiple Ethernet lines equally.

Bandwidth ratio: Connections are distributed to multiple Ethernet lines based on the bandwidth ratios of Ethernet lines.

Weighted minimum traffic: Connections are distributed preferably to the line with the smallest ratio of traffic to bandwidth.

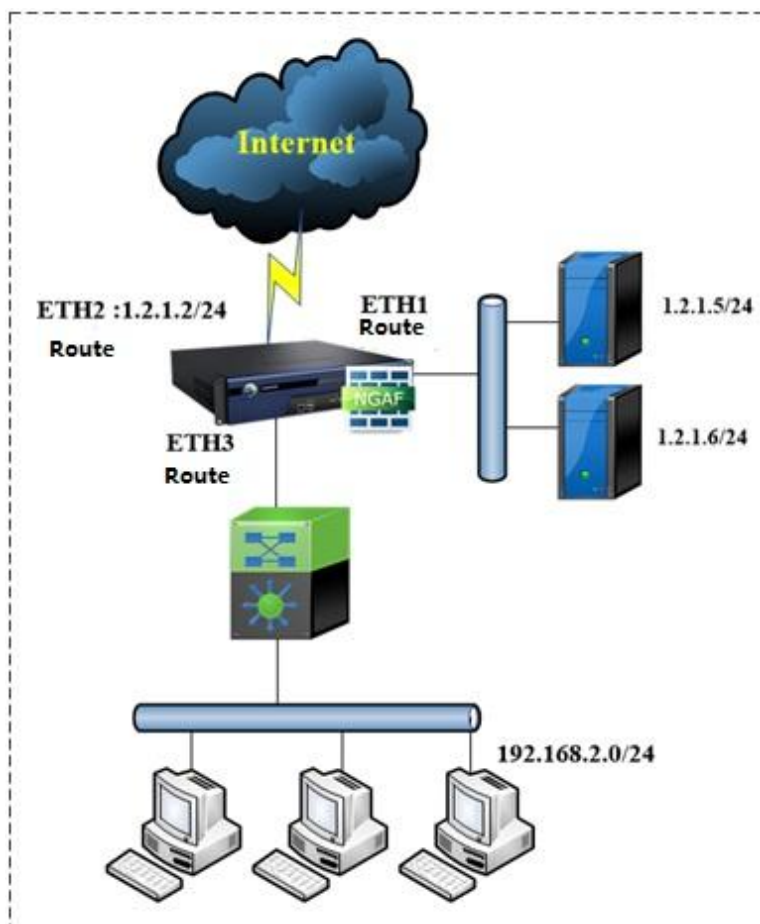
Preferred use of the preceding line: is used when lines work in active/standby mode. All connections are distributed to the first line. When the first line is faulty, connections are redistributed to the selected available line.



- To implement load balancing on multiple Ethernet lines, enable link failure detection. For details, see section 3.2.1.1.
- Only interfaces with WAN attributes can be used for multiline load balancing.
- Each Ethernet line must correspond to a PBR. The PBR can be based on the source IP address or multiline load balancing.

ARP Proxy Configuration

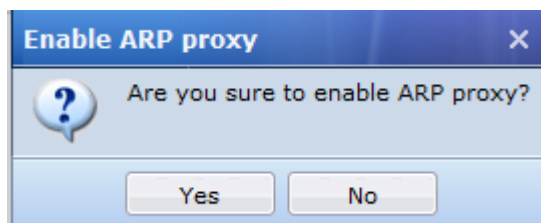
Configuration example: The following figure shows the network environment where the server cluster is deployed on the intranet and assigned with public IP addresses and the NGAF serves as a proxy to enable intranet users to access the Internet by using private IP addresses and to access intranet servers by using public IP addresses. ARP proxy must be implemented in non-hybrid deployment scenarios.



Step 1: Choose **Advanced Network Settings > ARP > ARP Proxy** and select **Enable ARP proxy**, as shown in the following table.

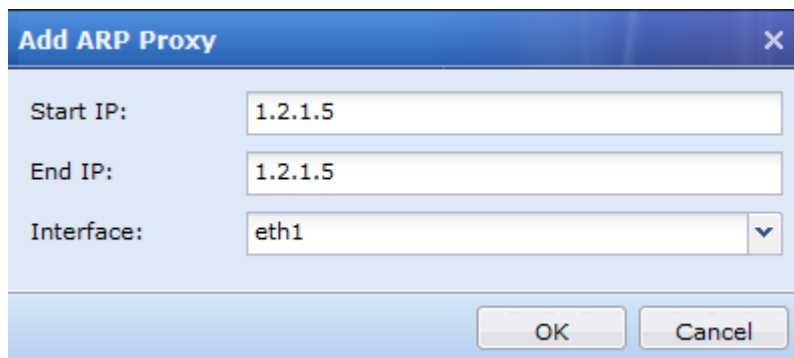
Advanced Network Settings					
ARP DNS DHCP SNMP					
ARP Protection << ARP Proxy					
> ARP Table					
> ARP Proxy					
<input checked="" type="checkbox"/> Enable ARP proxy					
+ Add X Delete Refresh					
<input type="checkbox"/> No. Start IP End IP Interface Status					

The following prompt is displayed.



Click **Yes**.

Step 2: Click **Add**. The **Add ARP Proxy** dialog box is displayed.



Start IP and **End IP**: specifies the IP address range of servers.

Interface: specifies the interface of the NGAF connected to servers. Set **Interface** to **eth1** (servers are connected to interface ETH1).

Click **OK**. Users can access servers on the intranet by using public IP addresses. No port mapping rule needs to be added on the NGAF.



The requirements described above can be met by deploying the NGAF in hybrid mode or deploying the NGAF as a router and configuring ARP proxy. When ARP proxy is used, (1) configure a public IP address for the Ethernet interface of the NGAF; (2) configure the interface of the NGAF connected to servers on the intranet as a router interface; (3) configure an IP address that does not conflict with IP addresses in other network segments for the router interface.

DHCP Configuration

Server Configuration

Configuration example: The intranet interface ETH2 of the NGAF is connected to intranet segments. The NGAF is required to automatically assign IP addresses 192.168.1.100 – 192.168.1.199 to users in a conference room to access the Internet. The fixed IP address 192.168.1.100 is assigned to the manager's PC.

Step 1: Enable the DHCP service.

Step 2: Select **eth2** in **Network Interface** for DHCP configuration. Set **Lease** and **DHCP Parameters**.

eth2

Lease (min): ⓘ

DHCP Parameters

Gateway:

Subnet Mask:

Preferred DNS:

Alternate DNS:

Preferred WINS:

Alternate WINS:

OK

Lease (min): specifies the use time of IP addresses.

DHCP parameters include **Gateway**, **Preferred DNS**, **Alternate DNS**, **Preferred WINS**, and **Alternate WINS**. The parameters are used when IP addresses are assigned through DHCP automatically.

Step 3: Set **IP Address Pool**, that is, the IP addresses to be assigned automatically.

IP Address Pool ⓘ

Step 4: Click **Reserved IP Addresses** to perform related setting so that a fixed IP address is assigned to a PC based on the corresponding MAC address.

Reserved IP Addresses

A MAC/host can only be assigned one IP address from the pool above.

Reserved IP Addresses

Click Add. The Reserved IP Addresses dialog box is displayed. Set Name, IP Address, MAC Address, Host Name, etc.

Reserved IP Addresses				
+ Add X Delete				
<input type="checkbox"/>	Name	IP Address	MAC Address	Host Name
<input type="checkbox"/>	John	192.168.1.118	F0-AC-12-13-14-BB	John-pc

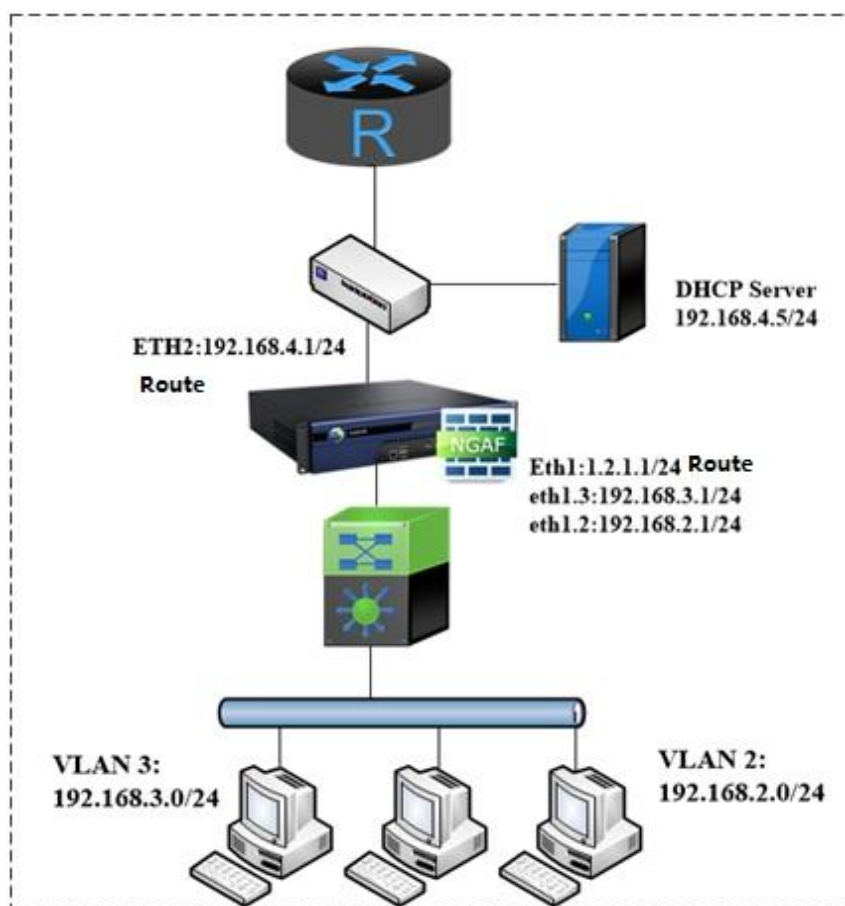
OK Cancel



To view the DHCP operating status and how IP addresses are assigned through DHCP, choose **Status > DHCP** from the navigation menu.

DHCP Relay Configuration

Configuration example: The following figure shows the network environment where the switch of the intranet is divided into multiple VLANs, which are assigned with IP addresses by a DHCP server. The NGAF must work as the gateway of VLANs on the intranet and as DHCP relay.



Step 1: Configure interfaces on the NGAF. Configure interfaces ETH1 and ETH2 as router interfaces and add the subinterfaces of VLAN2 and VLAN3 to interface ETH1. For interface configuration, see section 3.2.1.

Step 2: Select ☒ Enable DHCP relay .

Step 3: Set **Apply Relay to Selected Interfaces** and **DHCP Server**. In the **Apply Relay to Selected Interfaces** area, select the interfaces of the NGAF used to communicate with the DHCP server and client.

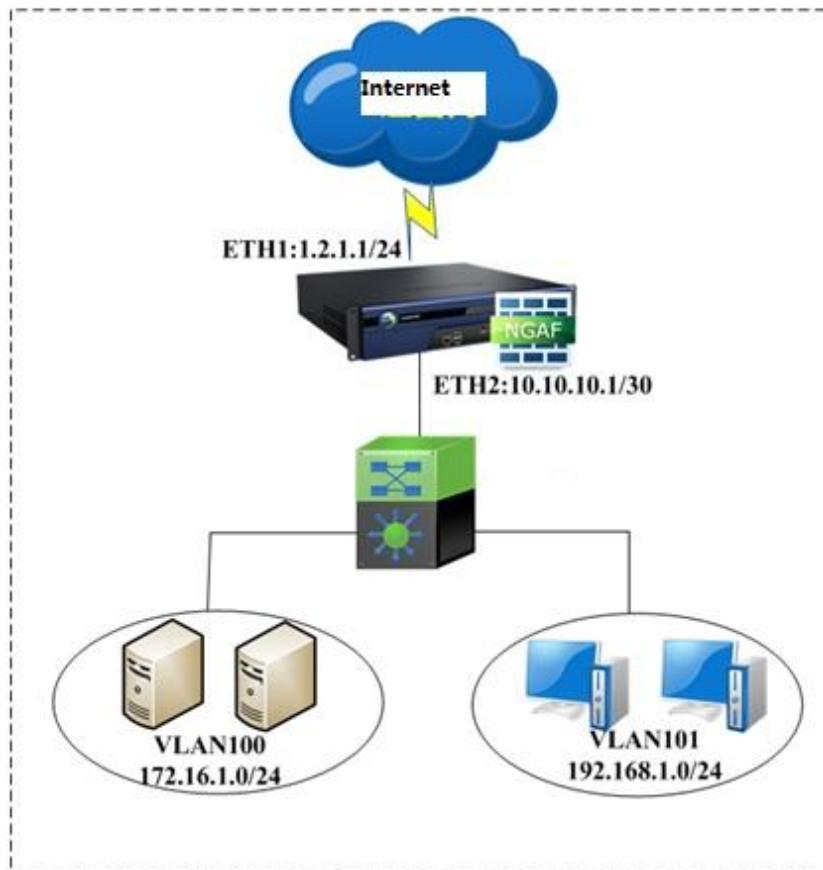
The screenshot shows the DHCP Relay configuration window. At the top, there are two tabs: 'DHCP Server' and 'DHCP Relay', with 'DHCP Relay' being the active tab. Below the tabs, there is a checkbox labeled 'Enable DHCP relay' which is checked. Underneath this, there is a section titled 'Apply Relay to Selected Interfaces'. This section contains two lists: 'Available:' on the left and 'Selected:' on the right. The 'Available:' list contains 'eth0', 'eth2', and 'eth3'. The 'Selected:' list contains 'eth1' and 'eth4'. Between these two lists are two buttons: 'Add' with a right-pointing arrow and 'Delete' with a left-pointing arrow. At the bottom of the window, there is a label 'DHCP Server:' followed by a text input field containing the IP address '127.0.0.1'.



DHCP relay supports all router interfaces, subinterfaces, and VLAN interfaces, but does not support router interfaces used for ADSL dial-up. If an interface enabled with DHCP relay is not connected, DHCP relay is affected.

Configuration of DoS/DDoS Protection

The following figure shows the network topology where the network segment of intranet servers is 172.16.1.0/24 and the network segment of intranet users is 192.168.1.0/24. The servers were once under DDoS attacks, causing application interruption. The servers and users on the intranet must be protected from attacks by means of DoS/DDoS protection. When an intranet user under an attack sends a large amount of sessions and data, the connection of the user is blocked to ensure network stability.



Step 1: Choose **Network > Interface > Zone** to define the zones of interfaces before configuring DoS protection. Choose **Objects > IP Group** and define the IP address group of servers on the intranet. For details, see section 3.5.7. Set **ETH2** to **LAN**, **ETH1** to **WAN**, and 172.16.1.0/24 to **Server Farm**.

Step 2: Choose **Firewall > Anti-DoS/DDoS > Outside Attack**. Set **Zone** to **WAN**, select **Defense against ARP flooding attack**, and set **Scan Prevention**.

Add Outside Attack Defense Policy

☒ Enable policy

Name:

Description:

Zone:

☒ Defense against ARP flooding attack

Per-Src-Zone Packets Threshold(packets/sec):

Scan Prevention ⓘ

☒ IP scan prevention

Threshold(packets/sec):

☒ Port scan prevention

Threshold(packets/sec):

OK Cancel

Step 3: Click **Select type** under **Defense Against DoS/DDoS Attack** to access the anti-attack configuration interface. Set **Dst IP** to **Server Farm**, select the attack detection types below, and click **OK**.

Dst IP:

☒ Defense against ICMP flooding attack

Per-Dst-IP Packet Threshold (packets/sec):

☒ Defense against UDP flooding attack

Per-Dst-IP Packet Threshold (packets/sec):

☒ Defense against SYN flooding attack

Per-Dst-IP Packet Threshold (packets/sec):

Per-Dst-IP Packet Loss Threshold (packets/sec):

Per-Src-IP Packet Loss Threshold (packets/sec):

☒ Defense against DNS flooding attack

Per-Dst-IP Packet Threshold (packets/sec):

Step 4: Select **Log event** and **Deny** in the **Action** area, leave **Packet-Based Attack** and **Abnormal Message Probe**

unspecified, and click **OK**.

The screenshot shows a configuration window for Anti-DDoS. It is divided into three main sections:

- Packet-Based Attack:** Contains a label "Attacks:" followed by a blue link that says "Selected: Unknown protocol,TearDrop atta...".
- Abnormal Message Probe:** Contains two labels: "Bad IP Options :" followed by a blue link "Select type", and "Bad TCP Options:" followed by a blue link "Select type".
- Action:** Contains two checkboxes: "Log event" (checked) and "Deny" (checked).

The screenshot shows the "Anti-DoS/DDoS" configuration window. The "Outside Attack" tab is selected. Below the tab are buttons: "+ Add", "X Delete", "✓ Enable", "✗ Disable", and "🔄 Refresh". Below these buttons is a table with the following columns: "No.", "Name", "Description", "Type", and "Attack Source Zone". The first row of the table has a checked checkbox in the "No." column.

No.	Name	Description	Type	Attack Source Zone
<input checked="" type="checkbox"/>				

Step 2: Choose **Firewall > Anti-DoS/DDoS > Inside Attack**. Set **Source Zone** to **LAN**, click **Only allow packets from the following sources**, and specify the network segments of servers and users on the intranet. Click **Connect to intranet through L3 switch** (a layer 3 switch is deployed). Set **IP Exclusion** to the network segment of servers. Click **OK**.

Outside Attack

Inside Attack

☒ Enable defense against inside attacks

Source Zone:

LAN

Source Address:

☐ Allow packets from any source

☒ Only allow packets from the following sources

172.16.1.0/255.255.255.0
192.168.1.0/255.255.255.0

Device Deployment:

☒ Connect to intranet through L3 switch

☐ Directly connect to intranet through L2 switch, no L3 switch in between

IP Exclusion:

(Packets from the following IP addresses will not be blocked)

172.16.1.0/255.255.255.0

Max TCP Connections:

1024

Max Attack Packets:

10240

Lockout Period (min):

3

Action

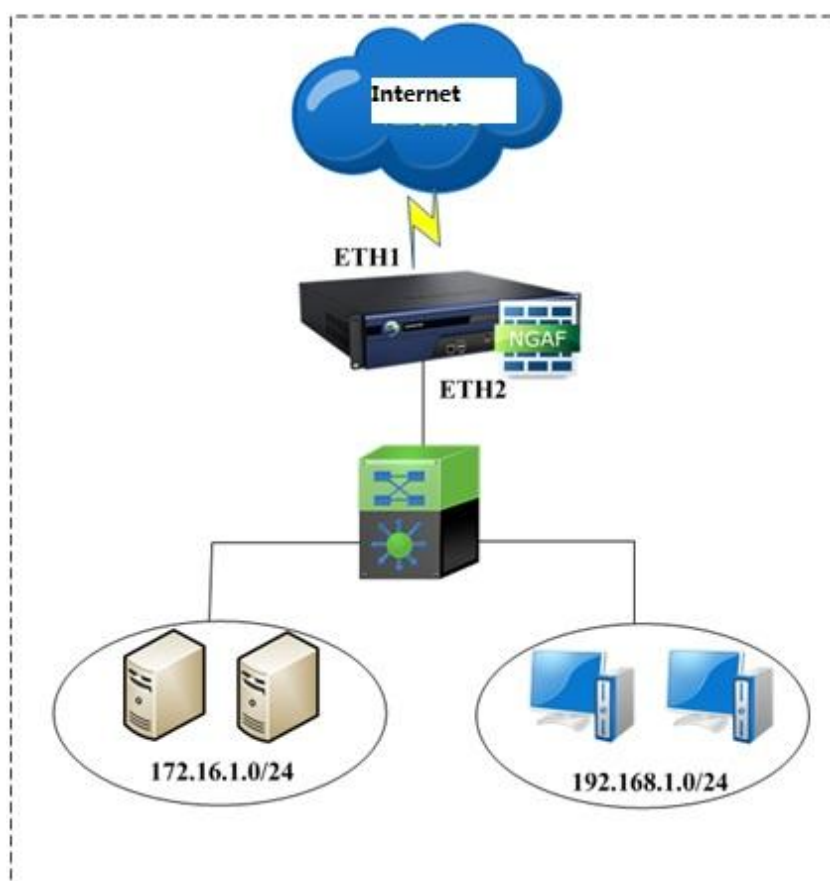
☒ Log event

OK

Access Control Configuration

Configuration of Application Control Policy

The following figure shows a network topology. The working efficiency of users on the intranet is low because they watch online videos and play games during work time. Users must be prevented from playing games and watching online videos during work time, but are allowed to do those things after work. The work time is 08:00–12:00 and 14:00–18:00.



Step 1: Define objects before configuring an application control policy. Choose **Network > Interface** and define the zones of interfaces. Choose **Objects > IP Group** and define the IP address group of servers on the intranet. Choose **Objects > Schedule** to define the work time of users. For details, see section 3.4.12.1. Set **ETH2** to **LAN**, **ETH1** to **WAN**, and **192.168.1.0/24** to **LAN IP Range**. Select **Working Hour** on the **Recurring Schedule** page.

IP Group

+ Add

✖ Delete

🔄 Refresh

📁 Import

📁 Export

<input type="checkbox"/>	No.	Name	Description	Delete
<input type="checkbox"/>	1	All	All IP addresses	In use
<input type="checkbox"/>	2	Server Farm		In use
<input type="checkbox"/>	3	Internal Users		✖
<input type="checkbox"/>	4	scansIPG20130815114346_000	The IP group is automatically generated during risk preven...	In use

Schedule

One-Time Schedule

Recurring Schedule

+ Add

✖ Delete

🔄 Refresh

<input type="checkbox"/>	No.	Name	Schedule	Description
<input type="checkbox"/>	1	All week	Mon - Sun;Morning 0:00 - Afternoon 11:59(the last minute included)	All week
<input type="checkbox"/>	2	Working Hour	Mon - Fri;Morning 8:00 - Morning 12:00	

Interfaces

Physical Interface

Sub-Interface

VLAN Interface

Aggregate Interface

Zone

Link State Propagation

+ Add

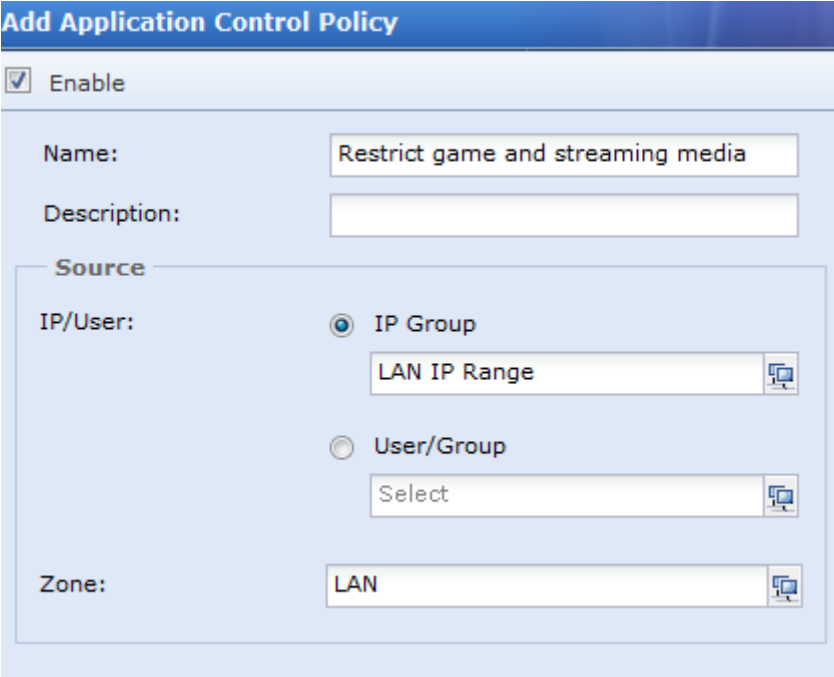
✖ Delete

🔄 Refresh

<input type="checkbox"/>	Zone Name	Zone Type	Interfaces	Device Mgt Privilege	Allowed Address	Delete
<input type="checkbox"/>	LAN	Route(layer 3)	eth2	WebUI,snmp	All	In use
<input type="checkbox"/>	WAN	Route(layer 3)	eth1	WebUI,snmp	All	In use

Step 2: Choose **Access Control > Application Control Policy** and click **Add**. The **Add Application Control**

Policy dialog box is displayed. Set **Name**, and set **Zone** to **LAN** and **IP Group** to **LAN IP Range** in the **Source** area.



Add Application Control Policy

☒ Enable

Name: Restrict game and streaming media

Description:

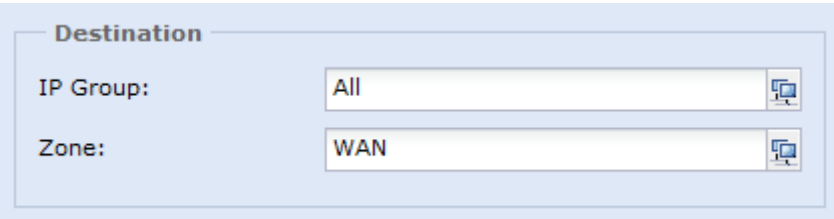
Source

IP/User: ☒ IP Group
LAN IP Range

☐ User/Group
Select

Zone: LAN

Step 3: In the **Destination** area, set **Zone** to **WAN** and **IP Group** to **All** (the destination IP addresses that are used when intranet users watch online videos and play games are unknown).



Destination

IP Group: All

Zone: WAN

Step 4: In the **Service/Application** area, set **Application** to **Streaming Media/All, Game/All, P2P** (online videos and games cannot be blocked on ports). Set **Schedule** to **Working Hour** and **Action** to **Deny**.

Service/Application

Service/Application: ☐ Service

☒ Application

Schedule:

Action: ☐ Allow ☒ Deny

Logging: ☐ Log event

Persistent Connection: ☐ Enable

Step 5: Click **OK**. The new policy is displayed on the **Application Control Policy** page.

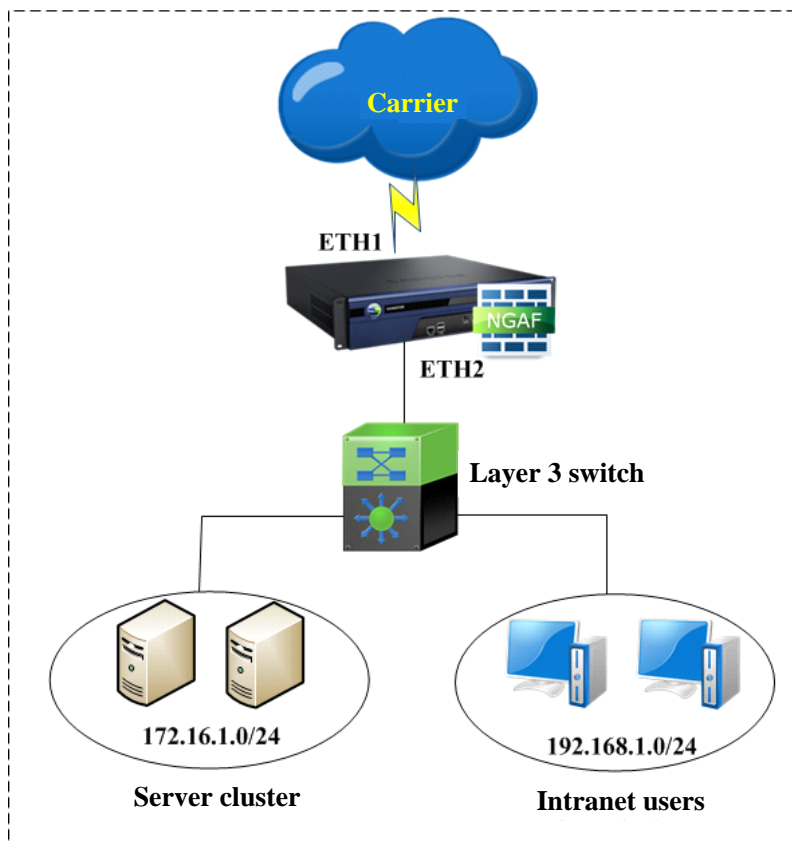
Application Control Policy										
<div> Add Delete Enable Disable Move Up Move Down Move Import </div> <div> Source Zone: <input type="text" value="All"/> Dst Zone: <input type="text" value="All"/> </div>										
No.	Name	Source Zone	Source IP/User	Dst Zone	Dst IP	Service/Application	Schedule	Action	Log...	Hit Co...
1	Restrict game a...	LAN	LAN IP Range 172.16.1.0/255.2...	WAN	All 0.0.0.0-255.255.2...	Streaming Media/All Game/All P2P Stream Media/All	All week	Deny	No	0



- The default policy of "Deny all" cannot be deleted because the firewall blocks all data by default. A policy for admitting data must be created.
- An IP address group must be configured in advance, or the IP address group can be set to a user group of the organization.

URL Filter Configuration

The following figure shows a network topology. Users on the intranet must be prevented from visiting illegal, pornographic, and reactionary websites.



Step 1: Choose **Network > Interface** and define the zones of interfaces before configuring a policy. Choose **Objects > IP Group** and define the IP address group of intranet users. For details, see section 3.4.8 Set **ETH2** to LAN, **ETH1** to WAN, and **192.168.1.0/24** to **LAN IP Range**.

IP Group					
+ Add X Delete Refresh Import Export					
<input type="checkbox"/>	No.	Name	Description	Delete	
<input type="checkbox"/>	1	All	All IP addresses	In use	
<input type="checkbox"/>	2	LAN IP Range		In use	

Interfaces					
Physical Interface Sub-Interface VLAN Interface Aggregate Interface Zone Link State Propagation					
+ Add X Delete Refresh					
<input type="checkbox"/>	Zone Name	Zone Type	Interfaces	Device Mgt Privilege	Allowed Address
<input type="checkbox"/>	LAN	Route(layer 3)	eth2	WebUI,snmp	All
<input type="checkbox"/>	WAN	Route(layer 3)	eth1	WebUI,snmp	All

Step 2: In the **URL Filter** dialog box, set **Name**, and set **Zone** to LAN and **IP Group** to LAN IP Range in the **Source** area (intranet users belong to a LAN).

URL Filter

☒ Enable

Name: Deny_access

Description:

Source

Zone: LAN

IP/User: ☒ IP Group
 LAN IP Range

☐ User/Group
 Select

Step 3: Select the types of websites that need to be filtered (embedded options). Set **Type** to **HTTPS (get)** and **HTTPS** (some illegal websites are accessed through HTTPS), **Schedule** to **All day**, and **Action** to **Deny**.

URL

URL Category: Adult Content, Pornography, Gambling

Type: ☒ HTTP(get)
☐ HTTP(post)
☒ HTTPS

Schedule: All week

Action: ☐ Allow ☒ Deny

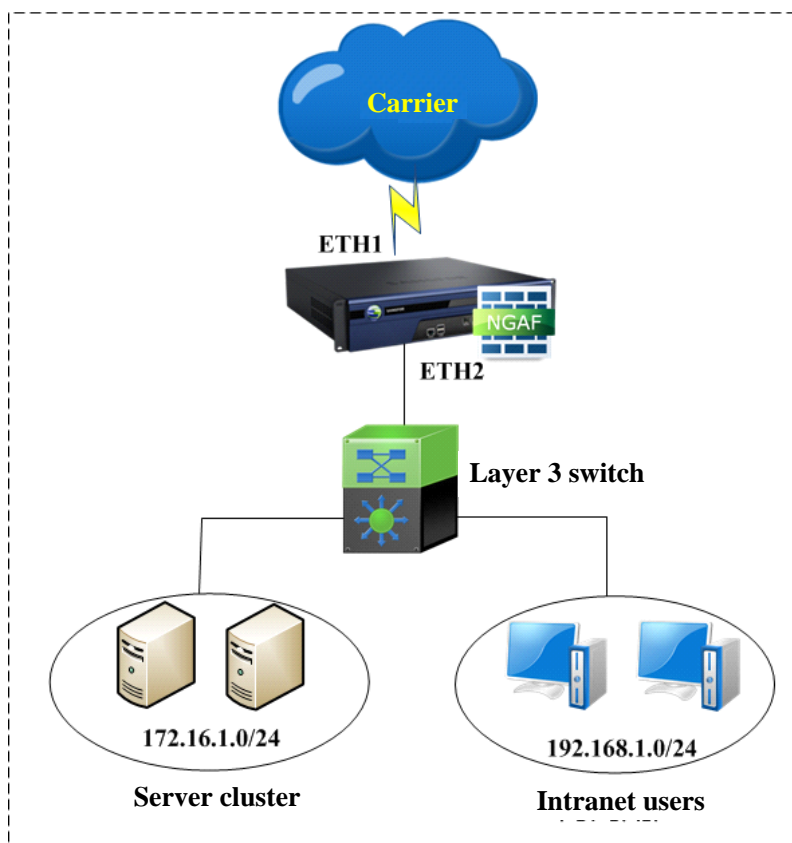
Logging: ☒ Log event

Save and Add Another OK Cancel

Click **OK**.

File Type Filter Configuration

The following figure shows a network topology. Users on the intranet must be prevented from downloading music and movies during work time. The work time is 08:00–12:00 and 14:00–18:00.



Step 1: Choose **Network > Interface** and define the zones of interfaces before configuring a policy. Choose **Objects > IP Group** and define the IP address group of intranet users. For details, see section 3.4.8. Set **ETH2** to **LAN**, **ETH1** to **WAN**, and **192.168.1.0/24** to **LAN IP Range**.

IP Group

No.	Name	IP Range	Description
1	All	0.0.0.0-255.255.255.255	All IP addresses
2	LAN IP Range	172.16.1.0/255.255.255.0	

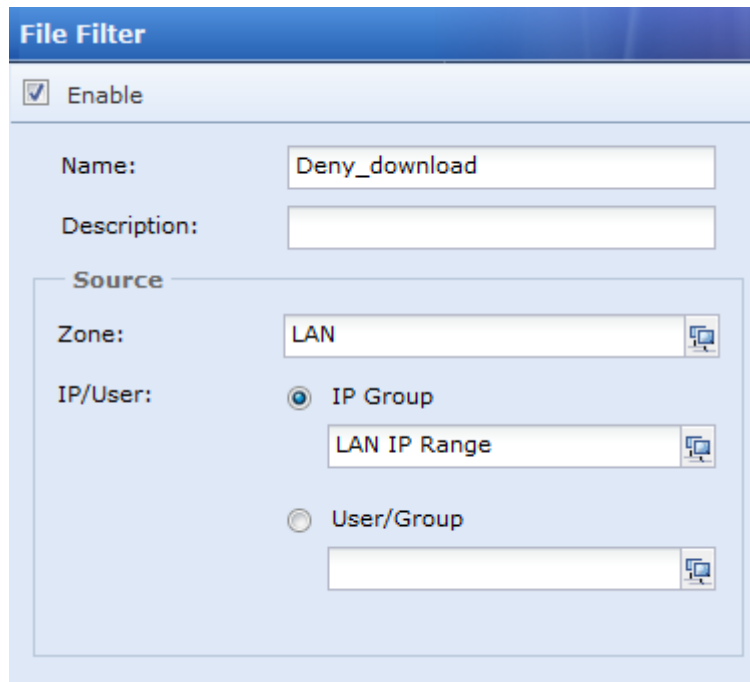
Interfaces

Zone Name	Zone Type	Interfaces	Device Mgt Privilege	Allowed Address
LAN	Route(layer 3)	eth2	WebUI,snmp	All
WAN	Route(layer 3)	eth1	WebUI,snmp	All

Schedule

No.	Name	Schedule	Description
1	All week	Mon - Sun;Morning 0:00 - Afternoon 11:59(the last minute included)	All week
2	Working Hour	Mon - Fri;Morning 9:00 - Afternoon 5:00	

Step 2: Access the **File Filter** dialog box. Set **Name**, and set **Zone** to **LAN** and **IP Group** to **LAN IP Range** in the **Source** area (intranet users access through interface ETH2 of the firewall).



File Filter

☒ Enable

Name:

Description:

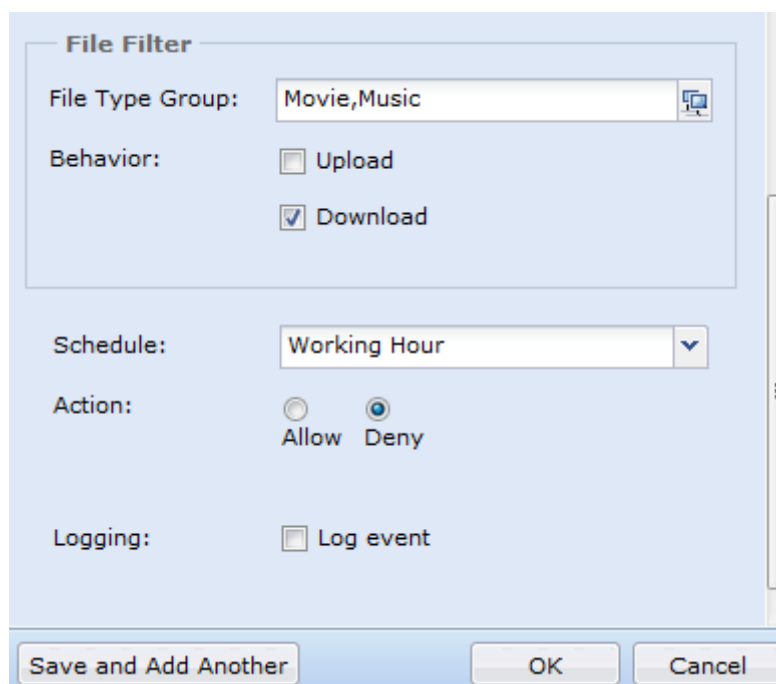
Source

Zone:

IP/User: ☒ IP Group

☐ User/Group

Step 3: In the **File Filter** area, set **File Type Group** to **Movie, Music** (embedded options), **Behavior** to **Download** (to prevent users from downloading), **Schedule** to **Working Hour**, and **Action** to **Deny**.



File Filter

File Type Group:

Behavior: ☐ Upload
☒ Download

Schedule:

Action: ☐ Allow ☒ Deny

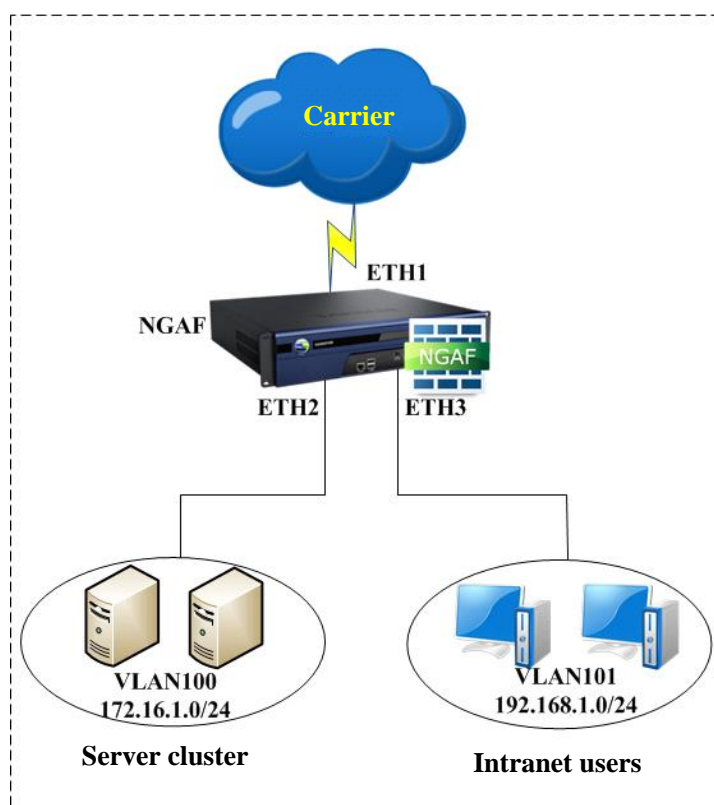
Logging: ☐ Log event

Save and Add Another OK Cancel

Click **OK**.

IPS Configuration

The following figure shows a network topology where the NGAF works as a router and the server cluster and user zone on the intranet are connected to two different interfaces of the firewall. Server and client protection must be implemented by the IPS function.



Step 1: Choose **Network > Interface** and allocate the three interfaces of the firewall to different zones. Set **ETH1** to **WAN**, **ETH2** to **DMZ**, and **ETH3** to **LAN**. Choose **Objects > IP Group**. Set **172.16.1.0/24** to **Server Farm** and **192.16.1.0/24** to **LAN IP Range**.

Interfaces				
Physical Interface	Sub-Interface	VLAN Interface	Aggregate Interface	Zone
+ Add X Delete Refresh				
Zone Name	Zone Type	Interfaces	Device Mgt Privilege	Allowed Address
- LAN	Route(layer 3)	eth3	WebUI,snmp	All
- WAN	Route(layer 3)	eth1	WebUI,snmp	All
- DMZ	Route(layer 3)	eth2	WebUI,snmp	All

IP Group			
+ Add X Delete Refresh Import Export			
No.	Name	Description	
- 1	All	All IP addresses	
- 2	Server Farm		
- 3	LAN IP Range		

Step 2: Configure server protection. Access the **IPS** page and click **Add**. The **Add IPS Rule** dialog box is displayed. Set **Name**, set **Zone** in the **Source** area to **WAN**, set **Zone** to **DMZ** and **IP Group** to **Server Farm** in the **Destination** area, select **Server** in the **Threat Prevention** area, select a rule, unselect **Endpoint**, and click **OK**.

Add IPS Rule

☒ Enable

Name:

Description:

Source

Zone:

Destination

Zone:

IP Group:

Threat Prevention

☒ Server Selected: worm,network_device,database

☐ Endpoint Selected: worm,file,backdoor,trojan,spyw

Action

Action: ☐ Allow ☒ Deny ⓘ

IP Lockout: ☐ Lock source IP

Logging: ☒ Log event

Save and Add Another
OK
Cancel

Step 3: Configure client protection. Access the **IPS** page and click **Add**. The **Add IPS Rule** dialog box is displayed. Set **Name**, set **Zone** to **WAN** in the **Source** area, set **Zone** to **LAN** and **IP Group** to **All** in the **Destination** area, select **Endpoint** in the **Threat Prevention** area, select vulnerabilities, and click **OK**.


Add IPS Rule

☒ Enable


Name:


Description:

Source

Zone: 

Destination

Zone: 


IP Group: 

Threat Prevention

☐ Server Selected: worm, network_device, database

☒ Endpoint Selected: worm, file, backdoor, trojan, spyware

Action

Action: ☐ Allow ☒ Deny 

IP Lockout: ☐ Lock source IP

Logging: ☒ Log event

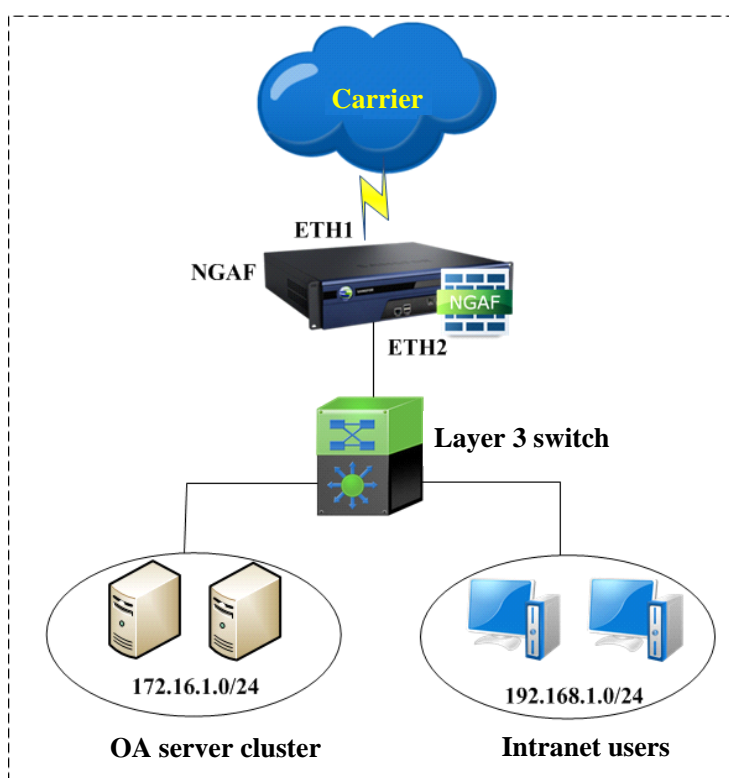


- The vulnerability protection rules of server protection and client protection are different because the types of attacks on the server and client are different.
- For server protection, the source zone is the zone of the Ethernet interface and the destination zone is the zone of the intranet interface. For client protection, the source zone is the zone of the intranet interface and the destination zone is the zone of the Ethernet interface.

Configuration of Web Application Protection

Example 1: WAF

The following figure shows a network topology where the NGAF is deployed as a router at the network egress. The web server cluster on the intranet must be protected. The protection includes hiding of FTP server version information, hiding of the **server** field and **VIA** field of web servers, OS command injection protection, SQL command injection protection, XSS command injection protection, CSRF command injection protection, HTTP abnormality detection, and buffer overflow detection. Only URLs containing "view" (http://www.***.com/view/) can be accessed. The service provision ports of servers on the intranet are WEB 80 and FTP 21.



Step 1: Choose **Network > Interface** and define the zones of interfaces before configuring a policy. Choose **Objects > IP Group** and define the IP address group of servers. For details, see section 3.4.8. Set **ETH2** to **LAN**, **ETH1** to **WAN**, and **172.16.1.0/24** to **Server Farm**.

IP Group			
+ Add X Delete Refresh Import Export			
<input type="checkbox"/>	No.	Name	Description
-	1	All	All IP addresses
<input type="checkbox"/>	2	Server Farm	
-	3	LAN IP Range	

Interfaces				
Physical Interface Sub-Interface VLAN Interface Aggregate Interface Zone Link State Propagation				
+ Add X Delete Refresh				
<input type="checkbox"/>	Zone Name	Zone Type	Interfaces	Device Mgt Privilege Allowed Address
-	LAN	Route(layer 3)	eth2	WebUI,snmp All
-	WAN	Route(layer 3)	eth1	WebUI,snmp All

Step 2: Access the **Web Application Protection** page and click **Add**. The **Add Web Application Protection Rule** dialog box is displayed. Set **Name** and set **Zone** in the **Source** area to **WAN** (the protected servers are on the intranet).

☒ Enable

Name:

Description:

Source

Zone:

Step 3: Set **Zone** to **LAN**, **IP Group** to **Server Farm**, and **Port** to **WEB 80** and **FTP21** in the **Destination** area. Keep other default ports.

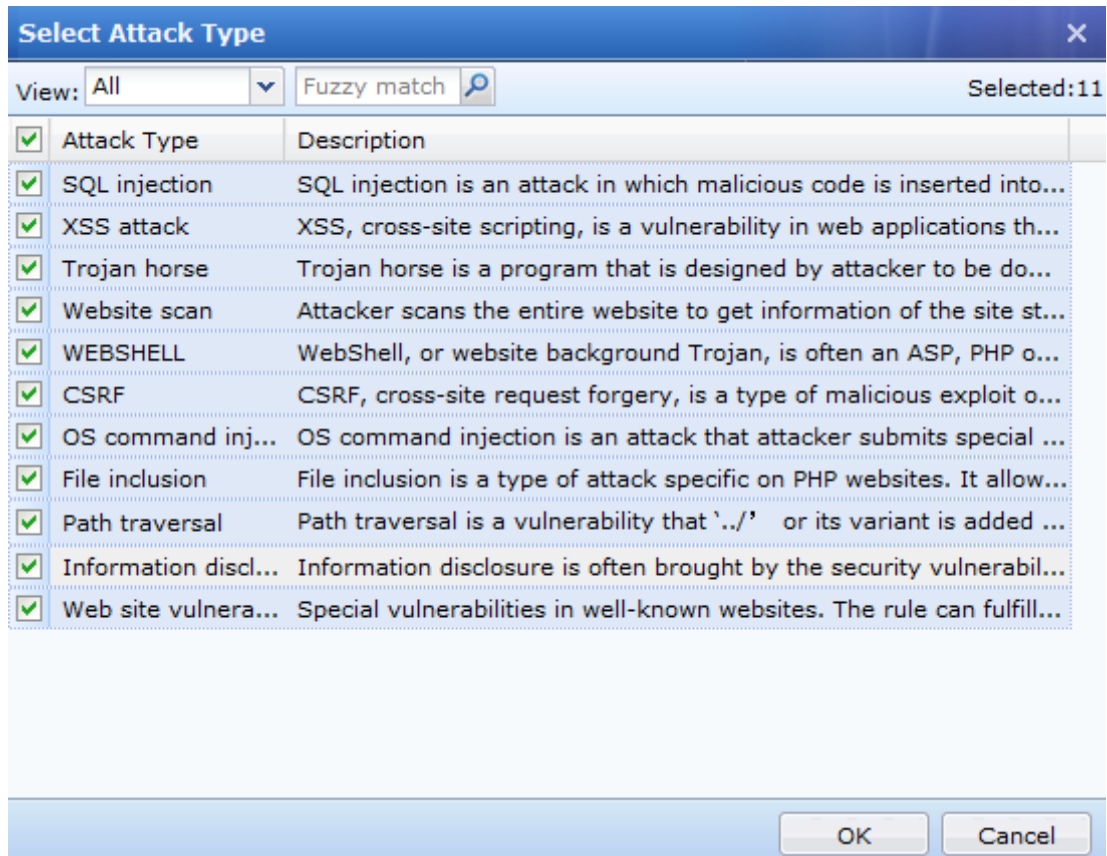
Destination

Zone:

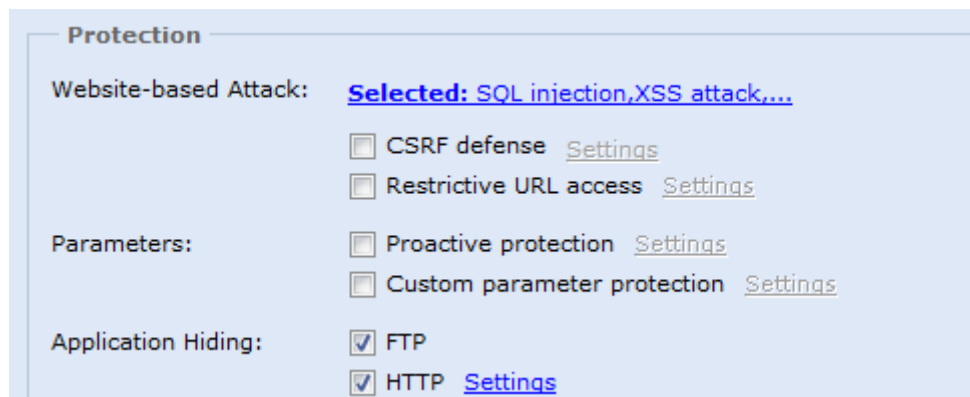
IP Group:

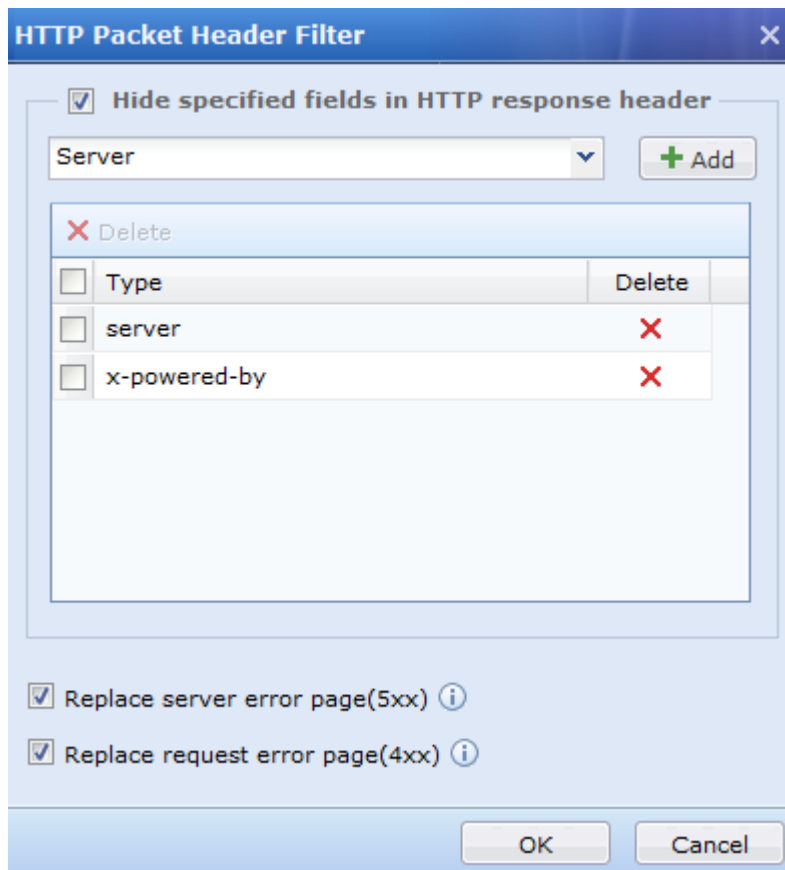
Port: [HTTP: 80; FTP: 21; MYSQL: 3306; TELNET: 23; ...](#)

Step 4: Select all attack types in the **Select Attack Type** dialog box.

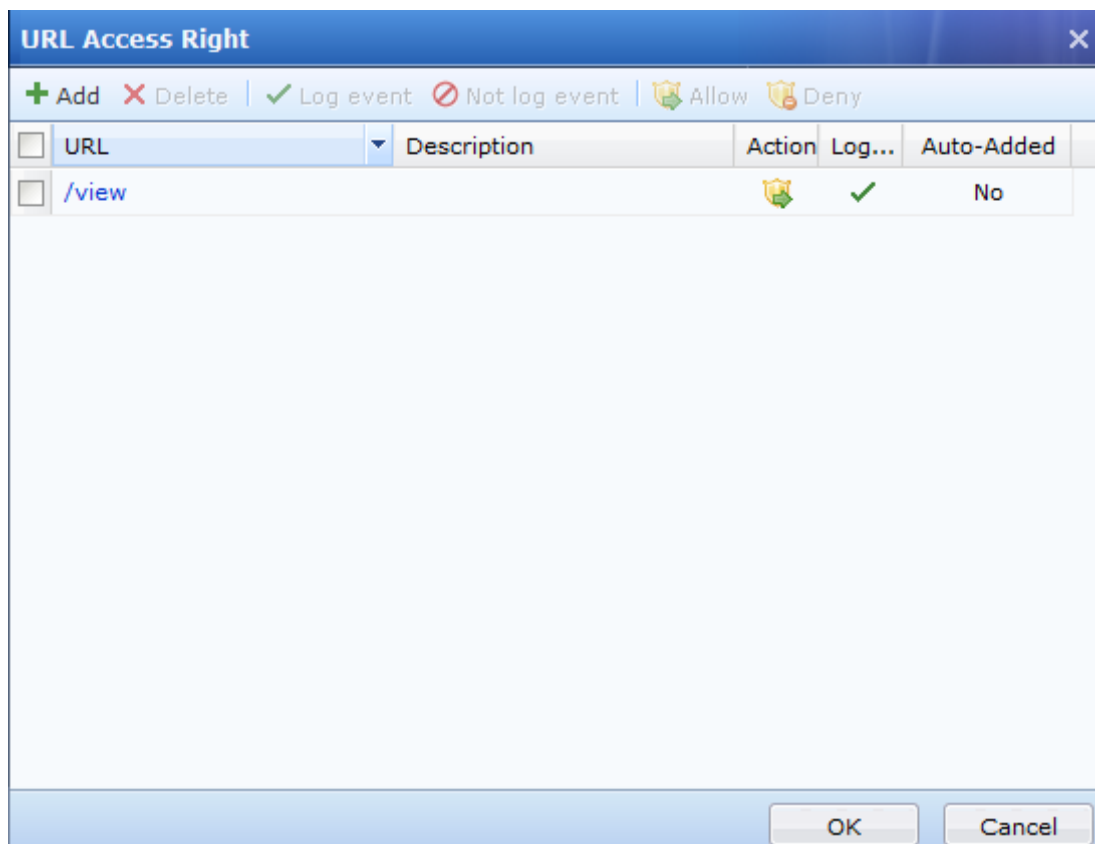


Step 5: Configure application hiding. Perform setting as shown in the following figures and click **OK** so that FTP server version information and the **server** field of the HTTP server are hidden.





Step 6: Select **URL Protection**, and click **Set**. Set **Action** to **Allow** for "view", indicating the URLs containing "view" are not checked.



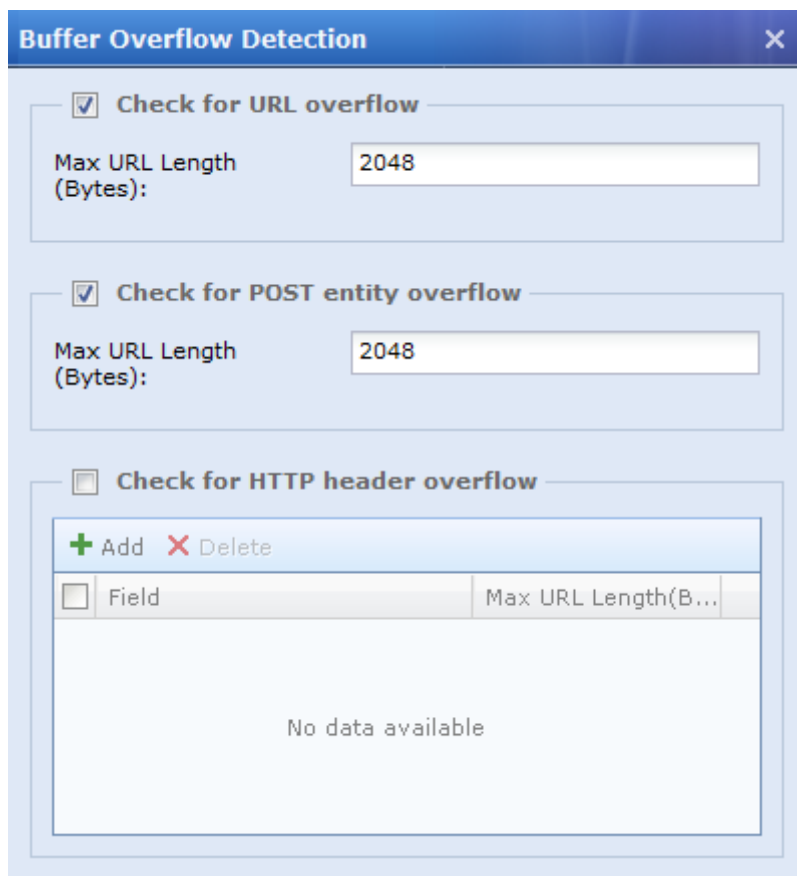
Step 7: Configure HTTP abnormality detection and buffer overflow detection. In the **Buffer Overflow Detection**

dialog box, select **Check for URL overflow** and **Check for POST entity overflow** and click **OK**.

HTTP:	<input checked="" type="checkbox"/> Protocol anomaly
	<input checked="" type="checkbox"/> Request method Settings
Website Scan:	Settings
Buffer Overflow:	Selected: URL overflow, POST entity overflow.

Allowed HTTP Request Method			
<input type="checkbox"/>	No.	Method	Description
<input checked="" type="checkbox"/>	1	GET	Send a "Display" request to the specified resou...
<input checked="" type="checkbox"/>	2	POST	Submit data (forms or files) to the specified res...
<input type="checkbox"/>	3	HEAD	It sends requests to the server for the specified...
<input type="checkbox"/>	4	OPTIONS	Make the server send back all the HTTP metho...
<input type="checkbox"/>	5	PUT	Upload the latest info to the specified resource
<input type="checkbox"/>	6	DELETE	Request the server for deleting resources with ...
<input type="checkbox"/>	7	TRACE	Display the requests received by the server, fo...
<input type="checkbox"/>	8	TRACK	For debugging the HTTP method of Web server ...
<input type="checkbox"/>	9	SEARCH	For searching resource
<input type="checkbox"/>	10	CONNECT	HTTP/1.1 protocol is reserved for the proxy ser...
<input type="checkbox"/>	11	PATCH	For partially modifying resource
<input type="checkbox"/>	12	DEBUG	For debugging or diagnose Web server, similar ...
<input type="checkbox"/>	13	PROPPATCH	This method can be used to set the attributes o...
<input type="checkbox"/>	14	PROPFIND	Retrieve the attributes of resources with Reque...
<input type="checkbox"/>	15	COPY	Request the server for duplicating the specified...

OK Cancel



Buffer Overflow Detection

☒ **Check for URL overflow**

Max URL Length (Bytes):

☒ **Check for POST entity overflow**

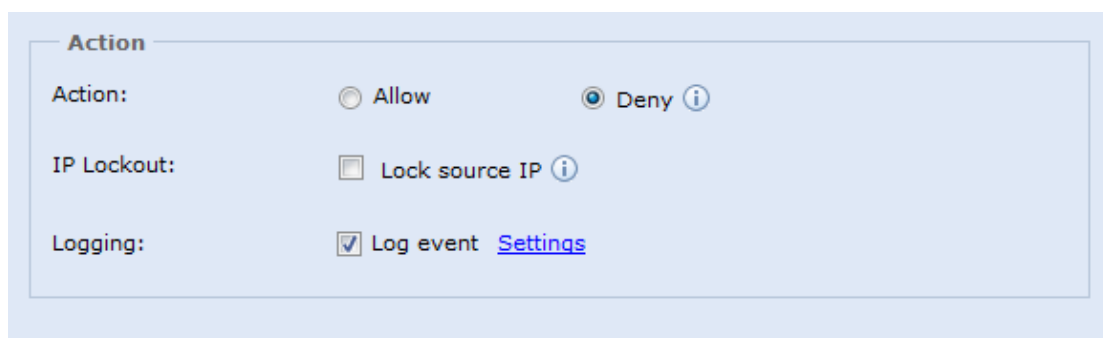
Max URL Length (Bytes):

☐ **Check for HTTP header overflow**

+ Add - Delete

<input type="checkbox"/> Field	Max URL Length(B...
No data available	

Step 8: Set **Action** to **Deny** and **Logging** to **Log Event** and click **OK**.



Action

Action: ☐ Allow ☒ Deny ⓘ

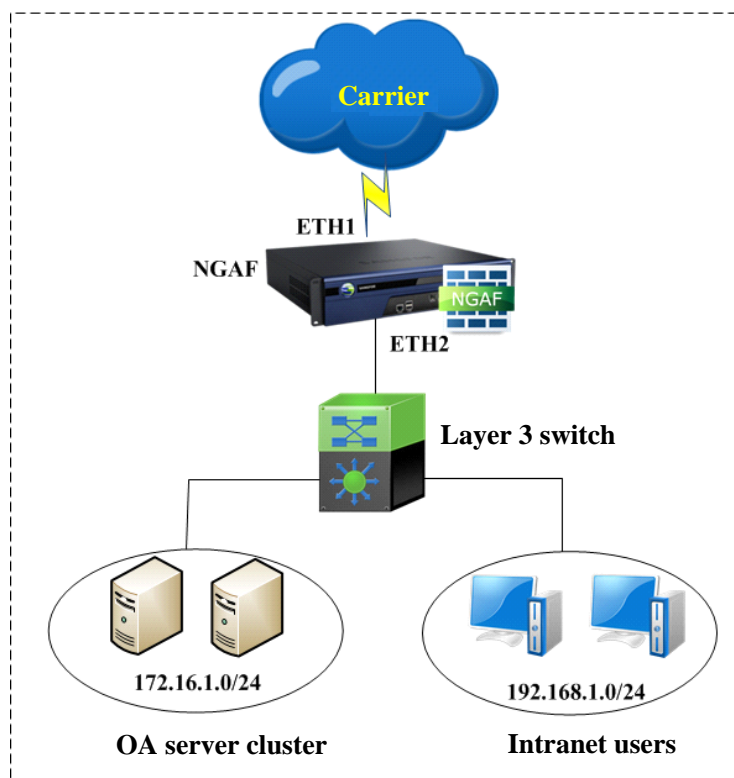
IP Lockout: ☐ Lock source IP ⓘ

Logging: ☒ Log event [Settings](#)

WAF							
+ Add - Delete ✓ Enable ✗ Disable ↑ Move Up ↓ Move Down ↔ Move 🔄 Refresh							
<input type="checkbox"/>	No.	Name	Source Zone	Dst Zone	Dst IP	Protection	Status
<input type="checkbox"/>	1	Server Prote...	WAN	LAN	Server Farm 10.0.0.0/24	Website-based Attack OS command injection,SQL injection,XSS attack,CSRF,Path trav... Application Hiding FTP,HTTP Password ...	✓

Example 2: Data Leak Protection

The following figure shows a network topology where the NGAF is deployed as a router at the network egress and a web server cluster is deployed on the intranet. The servers store the personal information of enterprise customers for users to query. The data must be protected to prevent leak of non-personal information to users. Bank account numbers, mobile phone numbers, and identity card numbers must not be contained in queried data, and files in **.doc** and **.xls** formats must not be downloaded from the servers.



Step 1: Choose **Network > Interface** and define the zones of interfaces before configuring a policy. Choose **Objects > IP Group** and define the IP address group of servers. For details, see section 3.4.8. Set **ETH2** to **LAN**, **ETH1** to **WAN**, and **172.16.1.0/24** to **Server Farm**.

IP Group

+ Add
- Delete
Refresh
Import
Export

No.	Name	Description
1	All	All IP addresses
2	Server Farm	
3	LAN IP Range	

Interfaces

Physical Interface
Sub-Interface
VLAN Interface
Aggregate Interface
Zone
Link State Propagation

+ Add
- Delete
Refresh

Zone Name	Zone Type	Interfaces	Device Mgt Privilege	Allowed Address
LAN	Route(layer 3)	eth2	WebUI,snmp	All
WAN	Route(layer 3)	eth1	WebUI,snmp	All

Step 2: Access the **Web Application Protection** page and click **Add**. The **Add Web Application Protection Rule** dialog box is displayed. Set **Name**, set **Zone** to **WAN** in the **Source** area (the protected servers are on the intranet), and set **Zone** to **LAN**, **IP Group** to **Server Farm**, and **Port** to **WEB 80** in the **Destination** area. Keep other default ports.

Add Web Application Protection Rule

☒ Enable

Name: DLP

Description:

Source

Zone: WAN

Destination

Zone: LAN

IP Group: Server Farm

Port: HTTP: 80; FTP: 21; MYSQL: 3306; TELNET: 23; ...

Step 3: Configure a sensitive data protection policy. When the data retrieved from a query contains bank accounts, mobile phone numbers, and identity card numbers, the query is considered as data leak.

Data Leak Protection

Data Leak Protection:
☒ Sensitive data protection [Settings](#)
☒ File download restriction [Settings](#)

[IP/URL Whitelist](#)

Sensitive Keyword Group [X]

Select Sensitive Keywords(the selected are with 'AND' logic):

<input type="checkbox"/>	No.	Sensitive Keyword	Regular Expression
Predefined Sensitive Keywords			
<input type="checkbox"/>	1	MD5	-
<input type="checkbox"/>	2	Eail address	-
Custom Sensitive Keywords			
<input checked="" type="checkbox"/>	3	ATM	100000000
<input checked="" type="checkbox"/>	4	IC	800000
<input checked="" type="checkbox"/>	5	Phone number	0100000000

Name:

Description:

Hit Count Threshold:

OK Cancel

Sensitive Data [X]

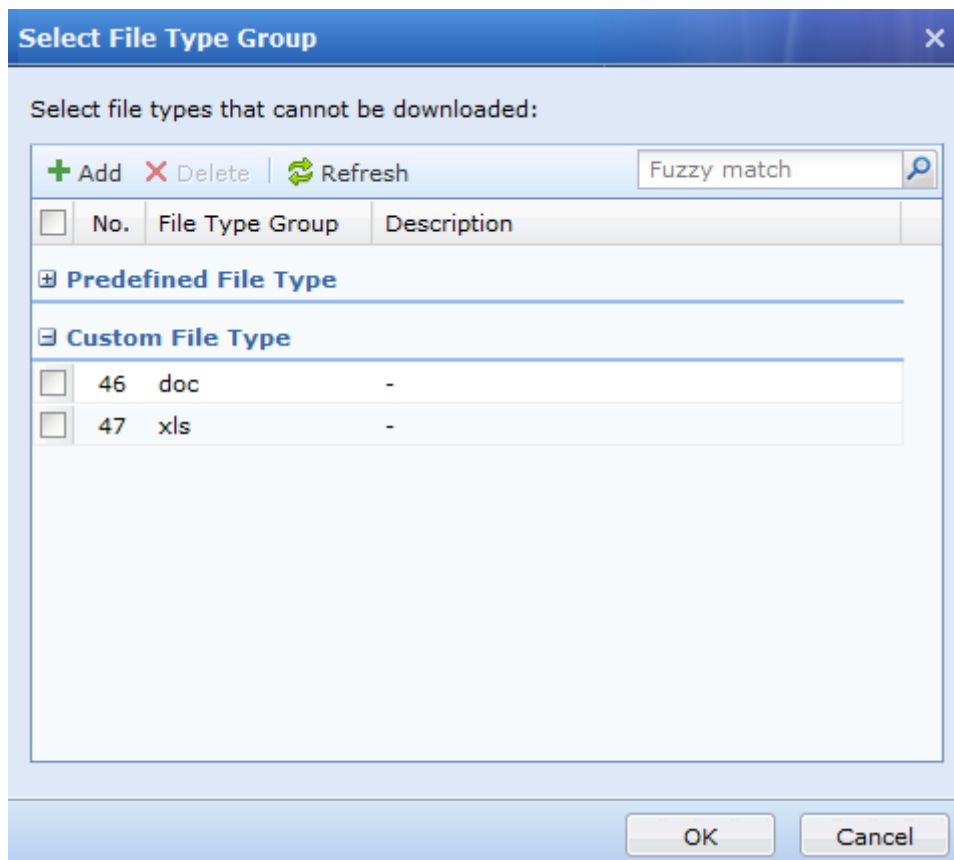
Hit Count Based On: [v] [i]

+ Add - Delete

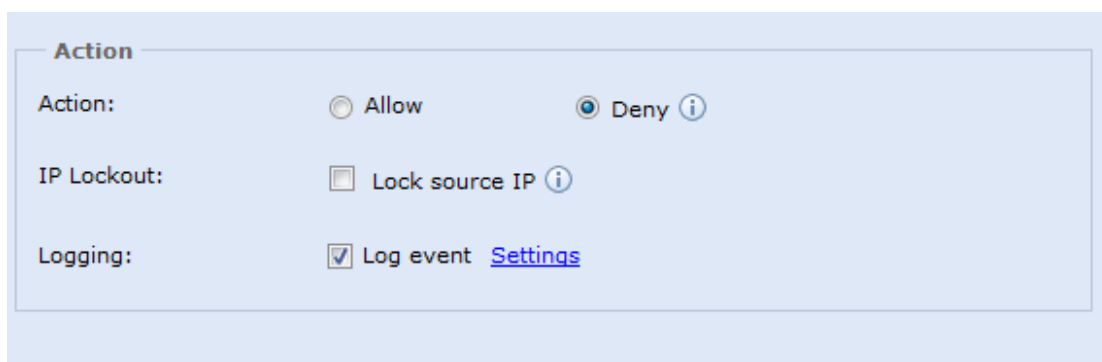
<input type="checkbox"/>	Sensitive Keyword ...	Description	Hit Count Threshold
<input type="checkbox"/>	DLP		1

OK Cancel

Step 4: Configure file downloading filter to prevent downloading files in .doc and .xls formats from servers.



Step 5: Set **Action** to **Deny** and **Logging** to **Log Event** and click **OK**.



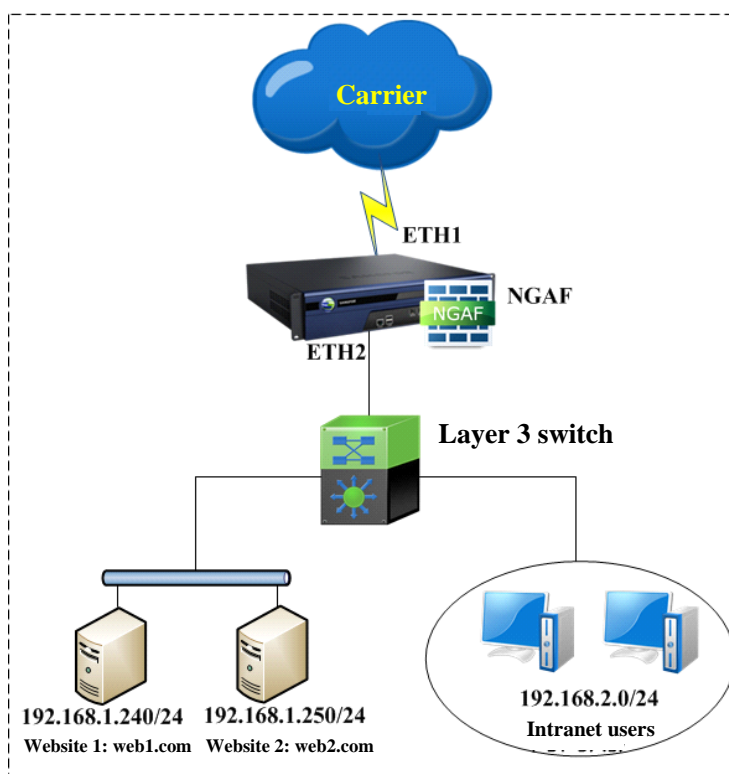
WAF						
+ Add -X Delete + Enable - Disable + Move Up - Move Down + Move + Refresh						
<input type="checkbox"/>	No.	Name	Source Zone	Dst Zone	Dst IP	Protection
<input checked="" type="checkbox"/>	1	DLP	WAN	LAN	Server Farm 10.0.0.0/24	Buffer Overflow URL overflow,Post entity overflow Data Leak Protection Sensitive data protection, File download restriction

Website Anti-defacement Configuration

The following figure shows a network topology where the NGAF works as a router and two web servers are deployed on the intranet. The following requirements must be met:

- The NGAF protects the web servers. When illegal defacement occurs, Internet users are prevented from visiting the defaced webpage and a prompt is displayed at the user end.

- Websites 1 and 2 are maintained by administrators 1 and 2 respectively. For example, administrator 1 logs in to an anti-defacement management system to update the local buffer after updating website 1.
- When website 1 is defaced, an email alarm (test1@domain.com) is sent to administrator 1. The email server uses the SMTP information of administrator@domain.com.
- When website 2 is defaced, an email alarm (test2@domain.com) is sent to administrator 2. The email server uses the SMTP information of administrator@domain.com.



Step 1: Perform basic network configuration. Configure the IP addresses and zones of the interfaces of the NGAF based on section 3.2 and section 5.1.1. Configure port mapping for the servers based on section 3.6.2.

Step 2: Choose **Server Security > Website Anti-Defacement**, select **Enable website anti-defacement**, and click **Webmaster** to add two webmaster accounts.

Website Anti-Defacement										
<input checked="" type="checkbox"/> Enable website anti-defacement										
+ Add X Delete ✓ Enable ✗ Disable 🔄 Update Local Cache ✎ Edit Multiple 👤 Webmaster 🔄 Refresh										
No.	Status	Website Name	Start URL	Website IP	Defaced Webpage	Cached Webpage	Whitelisted URL	Time	Time Cached	
1	Protected	CTI	http://sangforser...	1	0	428	0	-	2013-08-15 10:5...	

Add Webmaster

Username: admin1

Password:

Confirm:

☒ Allow to enable/disable anti-defacement

OK Cancel

Add Webmaster

Username: admin2

Password:

Confirm:

☒ Allow to enable/disable anti-defacement

OK Cancel

Step 3: Choose **System** > **SMTP Server** and set SMTP server information

SMTP Server Webmasters

Sender Address: Administrator@domain.com

SMTP Server: smtp.domain.com

☒ Require authentication

Username: Administrator ⓘ

Password:

Sent Test Email

OK

Step 4: Choose **Server Security** > **Website Anti-Defacement** and click **Add** to create two anti-defacement policies for websites 1 and 2.

Edit Website Anti-Defacement Rule [X]

Website Name:

Start URL:

Server IP: [Settings](#)

Max URL Levels: [↑] [↓] [i]

Detection Method: [v] [i]

☒ Check for resource file defacement [i]

☒ Check for unsafe links to virus/ads on defaced webpage

Action Taken if Defacement Detected

☒ Notify network administrator [i]

Email: [i]

☒ Block user from accessing website

☒ Redirect browser to prompt page

☐ Redirect browser to server address [i]

☒ Log event

☒ Allow admin to maintain this website

Webmaster: [i]

Portal: [Visit Now](#)

Website Server Address

+ Add

✖ Delete

[How to configure IP address list?](#)

<input type="checkbox"/>	Domain Name	IP Address
<input type="checkbox"/>	web1.com	192.168.1.240

OK

Cancel

Add Website Anti-Defacement Rule

Website Name:website2

Start URL:http://web2.com

Server IP:Settings

Max URL Levels:5

Detection Method:Fuzzy match - high sensitivity

☒ Check for resource file defacement

☒ Check for unsafe links to virus/ads on defaced webpage

Action Taken if Defacement Detected

☒ Notify network administrator

Email:test2@domain.com

Test

☒ Block user from accessing website

☒ Redirect browser to prompt page

Edit Webpage

☐ Redirect browser to server address

☒ Log event

☒ Allow admin to maintain this website

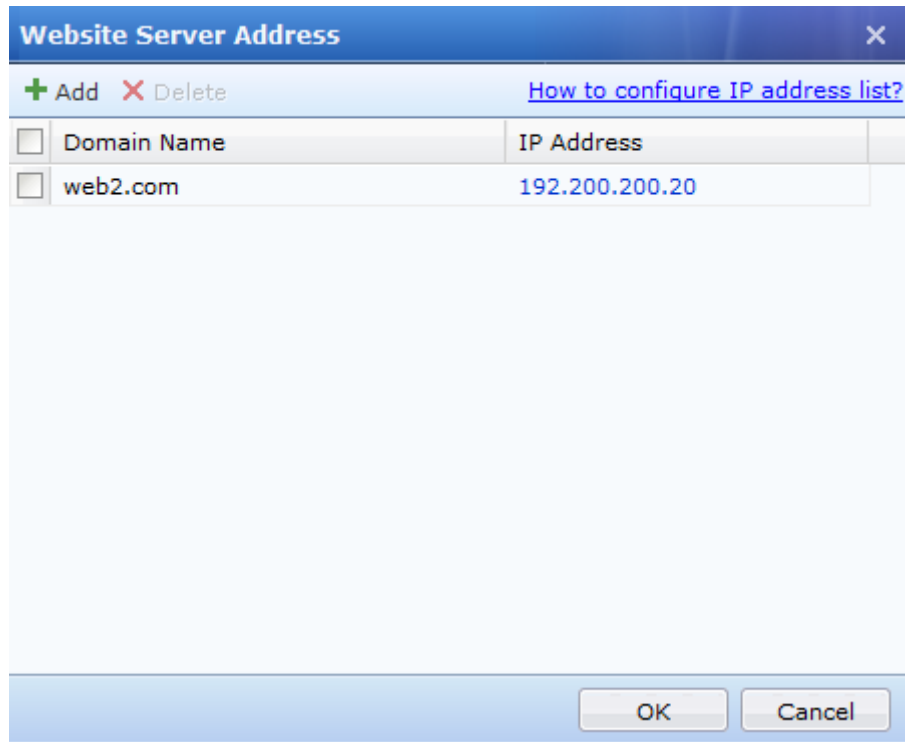
Webmaster:admin2

Portal:https://192.200.17.21:8000/guard.html Visit Now

Advanced

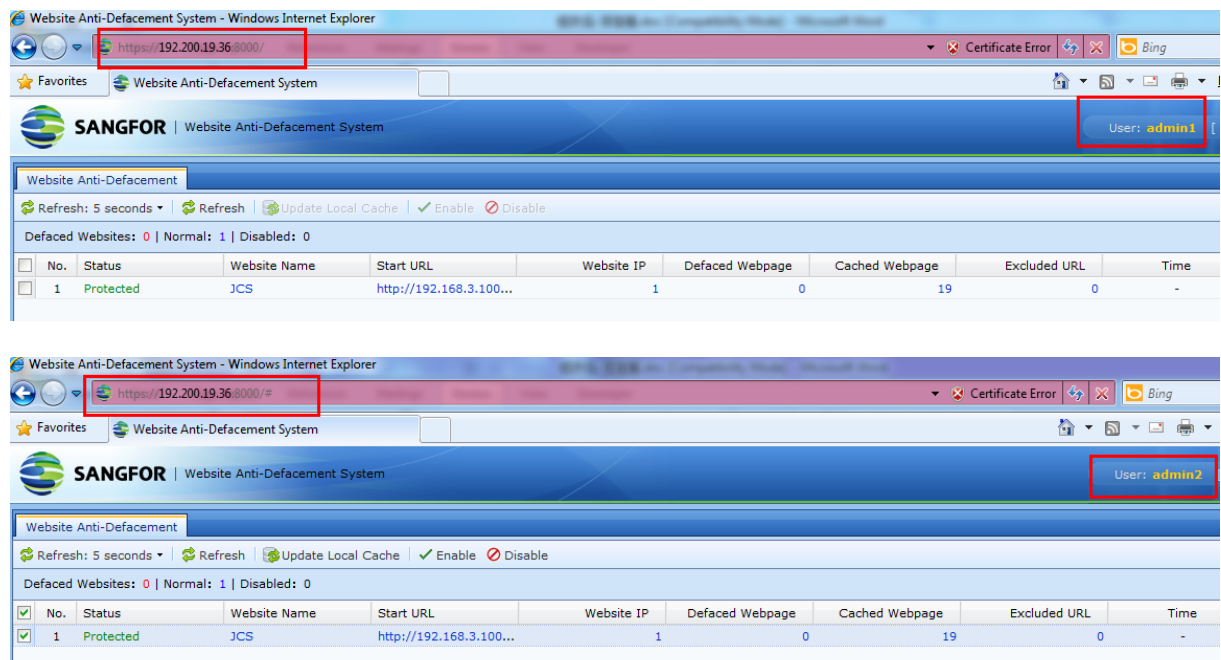
OK

Cancel



Website Anti-Defacement										
<input checked="" type="checkbox"/> Enable website anti-defacement										
<div><div><div><div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div></div></div></div></div>										

Step 5: Enable administrators 1 and 2 to log in through <https://device IP:8000> for management. The following figure shows the page after login.





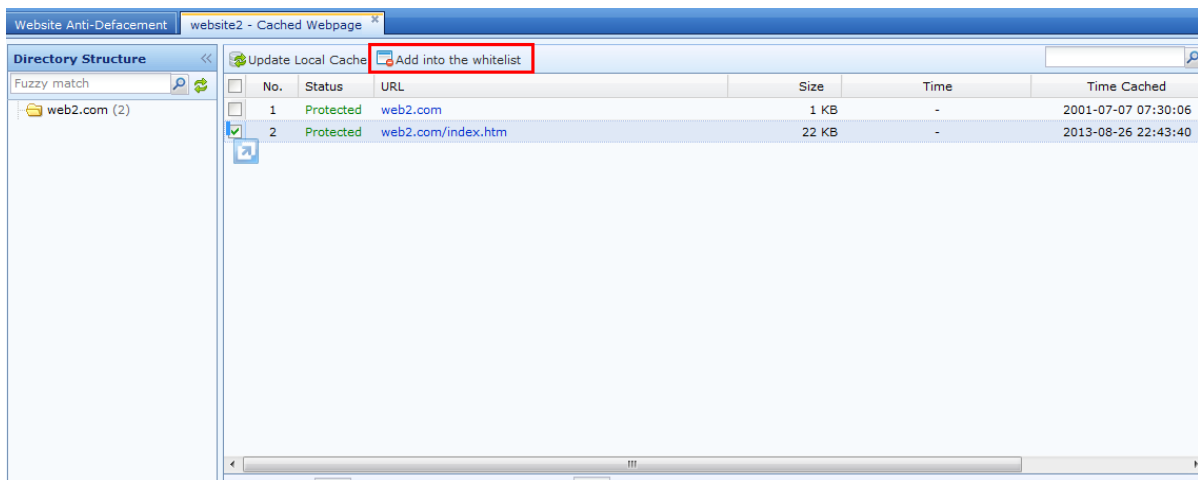
The configuration is completed. When defacement occurs, the following prompt is displayed at the user end.

Website under Maintenance...

This website is temporarily closed. Please try again later.

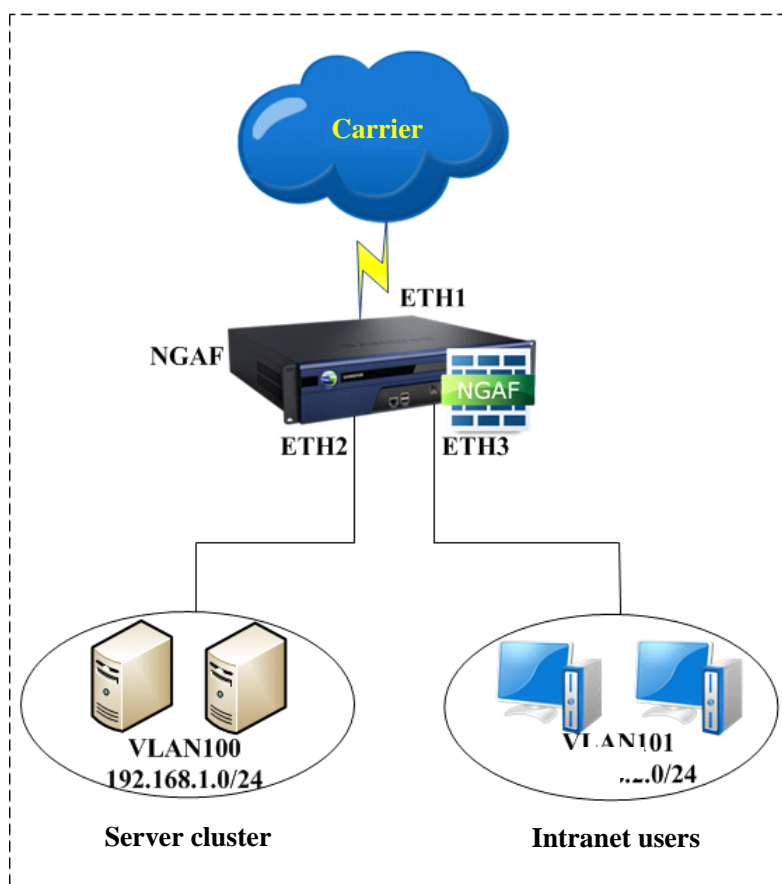


- To enable the NGAF to restore normally buffered pictures to the client end when only pictures are defaced, select ☒ Check defacement of static image/text file, etc. .
- To exclude a webpage from the defacement detection of the NGAF, click  Add into the whitelist.



Risk Assessment

The following figure shows a network topology where the NGAF works as a router and the server cluster and user zone on the intranet are connected to two different interfaces of the firewall. An administrator needs to know the enabled ports and vulnerabilities of the server with the IP address 192.168.1.249 and whether any weak password containing **sangfor** exists.



Step 1: Choose **Network > Interface** and define the zones of interfaces before configuring a policy. Choose **Objects > IP Group** and define the IP address group of servers. For details, see section 3.4.8. Set **ETH1** to **WAN**, **ETH2** to **DMZ**, **ETH3** to **LAN**, and **192.168.1.249** to **249**.

IP Group			
+ Add X Delete Refresh Import Export			
<input type="checkbox"/>	No.	Name	IP Range ^
<input type="checkbox"/>	1	All	0.0.0.0-255.255.255.255
<input type="checkbox"/>	2	Server Farm	10.0.0.0/24
<input type="checkbox"/>	3	LAN IP Range	172.16.1.0/255.255.255.0
<input type="checkbox"/>	4	249server	192.168.1.249

Interfaces				
Physical Interface Sub-Interface VLAN Interface Aggregate Interface Zone Link State Propagation				
+ Add X Delete Refresh				
<input type="checkbox"/>	Zone Name	Zone Type	Interfaces	Device Mgt Privilege
<input type="checkbox"/>	LAN	Route(layer 3)	eth3	WebUI,snmp
<input type="checkbox"/>	WAN	Route(layer 3)	eth1	WebUI,snmp
<input type="checkbox"/>	DMZ	Route(layer 3)	eth2	WebUI,snmp

Step 2: Configure an application control policy. Choose **Access Control > Application Control Policy** and enable all services used by intranet users to access servers and the HTTP service used by Internet users to access servers.

Application Control Policy										
Add Delete Enable Disable Move Up Move Down Move Import										
		Source Zone	All		Dst Zone	All				
No.	Name	Source Zone	Source IP/User	Dst Zone	Dst IP	Service/Application	Schedule	Action	Log...	Hit Co...
1	external access...	WAN	All 0.0.0.0-255.255.2...	DMZ	249server 192.168.1.249	Predefined Service/http	All week	Allow	No	0
2	internal access ...	LAN	All 0.0.0.0-255.255.2...	DMZ	249server 192.168.1.249	Predefined Service/any	All week	Allow	No	0

Step 3: Configure port scanning. On the **Risk Assessment** page, set **Untrusted Source Zone** to **WAN** and **LAN**, **Destination** to **192.168.1.249**, and **Port** to the frequently used port embedded in the NGAF.

Risk Assessment

Untrusted Source Zone:

WAN,LAN

Destination:

192.168.1.249

Specified Port:

80,81,8001,8002/http, 443...

Start

☐ Enable weak password scan

[Avoid Risk](#)
[Export as PDF](#)
[Clear Scan Results](#)
[All Associated Policies](#)

☐ Server IP
 Port
 Applic...
 Protocol
 Accessibl...
 Accessible IP
 Th

Step 4: Configure weak password scanning. On the **Risk Assessment** page, select **Enable weak password scan**, set **Range** to the default value and **Method** to **Full password dict**, and click **Advanced Settings**. In the **Advanced Settings** dialog box, set **Username Dictionary** to **sangfor**.

Enable weak password scan

Range:

ftp, mysql, mssql, netbio...

Method:

Full password dict (takes longer time)

Advanced Settings

OK

Cancel

Advanced Settings

RDP/VNC Service

RDP/VNC scan and full scan takes longer time. By default, it implements general scan.
☒ Implement full scan

Username/Password Dictionaries

Username Dictionary: ⓘ

sangfor


Password Dictionary: ⓘ

Type here

OK

Cancel



Step 5: Click  to start scanning. The following figure shows the scanning result.

Risk Assessment									
<div>Completed 96%</div> <div>Scanned 5312 ports, 1 ports left View Weak Password Details</div> <div>Tips: You may leave this page and check it again later.</div> <div> <div>Restart</div> <input checked="" type="checkbox"/> Enable weak password scan </div>									
<div> <div> <div>Avoid Risk</div> <div>Export as PDF</div> <div>All Associated Policies</div> </div> <div>All</div> <div>IP address or port</div> </div>									
Server IP	Port	Applic...	Protocol	Accessibl...	Accessible IP	Threat Le...	Risk		Operation
<input type="checkbox"/> 192.200.17.22	3306	mysql	TCP	WAN	0.0.0.0-255.255.255.255	High	Open port risk		
<input type="checkbox"/> 192.200.17.202	69	tftp	UDP	WAN	0.0.0.0-255.255.255.255	High	Open port risk		
<input type="checkbox"/> 192.200.17.202	21	ftp	TCP	WAN	0.0.0.0-255.255.255.255	High	Weak password risk1	Open port risk	
<input type="checkbox"/> 192.200.17.200	1433	mssql	TCP	WAN	0.0.0.0-255.255.255.255	High	Open port risk		
<input type="checkbox"/> 192.200.17.22	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	Open port risk	
<input type="checkbox"/> 192.200.17.203	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	Open port risk	
<input type="checkbox"/> 192.200.17.210	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	Open port risk	
<input type="checkbox"/> 192.200.17.202	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	Open port risk	
<input type="checkbox"/> 192.200.17.10	53	dns	UDP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk		
<input type="checkbox"/> 192.200.17.10	445	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk		

Move the cursor to a risk to view details.

<div><div><div>Avoid Risk</div><div>Export as PDF</div><div>All Associated Policies</div></div></div>							<div><div>All</div><div>IP address or port</div></div>		<div>Q</div>
<div><input type="checkbox"/></div>	Server IP	Port	Applic...	Protocol	Accessibl...	Accessible IP	Threat Le...	Risk	Operation
<div><input type="checkbox"/></div>	192.200.17.22	3306	mysql	TCP	WAN	0.0.0.0-255.255.255.255	High	Open port risk	
<div><input type="checkbox"/></div>	192.200.17.202	69	tftp	UDP	WAN	0.0.0.0-255.255.255.255	High	Open port risk	
<div><input type="checkbox"/></div>	192.200.17.202	21	ftp	TCP	WAN	0.0.0.0-255.255.255.255	High	Weak password risk1	Open port risk
<div><input type="checkbox"/></div>	192.200.17.200	1433	mssql	TCP	WAN	0.0.0.0-255.255.255.255	High	Open port risk	
<div><input type="checkbox"/></div>	192.200.17.22	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	Open port risk
<div><input type="checkbox"/></div>	192.200.17.203	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vul	
<div><input type="checkbox"/></div>	192.200.17.210	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vul	
<div><input type="checkbox"/></div>	192.200.17.202	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vul	
<div><input type="checkbox"/></div>	192.200.17.10	53	dns	UDP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<div><input type="checkbox"/></div>	192.200.17.10	445	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	

Page 1 of 1

Entries Per Page: 50

1-28 of 28

The port is prone to Web vulnerability, i, SQL injection, XSS attack, Trojan horse, Website scan, webshell, CSRF, OS command injection, File inclusion, Path traversal, Information disclosure

Step 6: Eliminate risks based on scanning prompts.

(1) Change weak passwords.

Completed 96%

Restart

Scanned 5312 ports, 1 ports left

[View Weak Password Details](#)

Tips: You may leave this page and check it again later.

☒ [Enable weak password scan](#)

Avoid Risk

Export as PDF

All Associated Policies

All

IP address or port


<input type="checkbox"/>	Server IP	Port	Applic...	Protocol	Accessibl...	Accessible IP	Threat Le...	Risk	Operation
<input type="checkbox"/>	192.200.17.22	3306	mysql	TCP	WAN	0.0.0.0-255.255.255.255	High	Open port risk	
<input type="checkbox"/>	192.200.17.202	69	tftp	UDP	WAN	0.0.0.0-255.255.255.255	High	Open port risk	
<input type="checkbox"/>	192.200.17.202	21	ftp	TCP	WAN	0.0.0.0-255.255.255.255	High	Weak password risk1	Open port risk
<input type="checkbox"/>	192.200.17.200	1433	mssql	TCP	WAN	0.0.0.0-255.255.255.255	High	Port is prone to weak password vulnerability	
<input type="checkbox"/>	192.200.17.22	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	Open port risk
<input type="checkbox"/>	192.200.17.203	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	Open port risk
<input type="checkbox"/>	192.200.17.210	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	Open port risk
<input type="checkbox"/>	192.200.17.202	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	Open port risk
<input type="checkbox"/>	192.200.17.10	53	dns	UDP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.10	445	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	

Page 1 of 1

Entries Per Page: 50

1-28 of 28

Change weak passwords based on risk prompts.

(2) Disable unnecessary ports. The scanning result shows the ports enabled on a server. Unnecessary ports can be disabled manually by a user with administrator rights. For example, to disable port 445 of the server with the IP address 192.168.1.249 used by intranet users to access the server, click  in the corresponding rule. The following dialog box is displayed.

Port Block Policy [X]

Source

Source Zone: WAN

Source IP: 0.0.0.0-255.255.255.255

Service

Target Server: 192.200.17.22

Service: TCP/3306

Action: Deny

Logging: Log event

OK Cancel

Click **OK**. The following information is displayed.

Risk Assessment

Untrusted Source Zone: WAN

Destination: 192.200.17.1-192.200.17.254

Port: 80,81,8001,8002/http, 443...

☒ Enable weak password scan

☒ Avoid Risk [All Associated Policies](#)

Server IP	Port	Applic...	Protocol	Accessibl...	Accessible IP	Threat Le...	Risk	Operation
192.200.17.202	23	telnet	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	⚠
192.200.17.200	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	⚠
192.200.17.210	443	https	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	⚠
192.200.17.232	3389	rdp	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	⚠
192.200.17.254	53	dns	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	⚠
192.200.17.254	443	https	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	⚠
192.200.17.232	445	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	⚠
192.200.17.232	139	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	⚠
192.200.17.107	139	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	⚠
192.200.17.22	3306	mysql	TCP	WAN	0.0.0.0-255.255.255.255	No risk	Port is in protection	✅

An application control policy is created automatically to prevent intranet users from visiting port 445 of the server with the IP address 192.168.1.249.

Application Control Policy

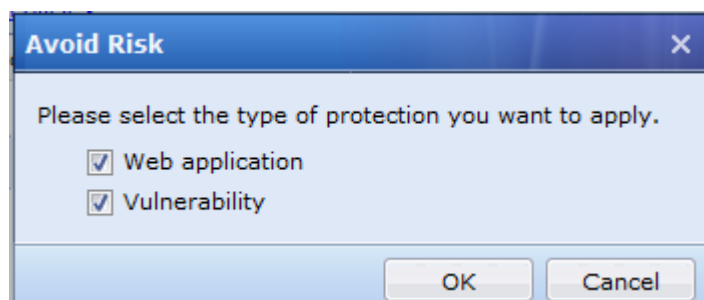
Source Zone: All Dst Zone: All

No.	Name	Source Zone	Source IP/User	Dst Zone	Dst IP	Service/Application	Schedule	Action	Log...	Hit Co...	Status	Clone	Del...
1	scansApp20130... The policy is au...	WAN	All 0.0.0.0-255.255.2...	WAN	scansIPG20130827... 192.200.17.22	Predefined Service/...	All week	Deny	Yes	0	✓	📄	✕
2	test	scansApp20130827105718_000 WAN	0.0.0.0-255.255.2...	WAN LAN WAN_TEST	All 0.0.0.0-255.255.2...	Predefined Service/any	All week	Allow	Yes	9999+	✓	📄	✕
3	Default Policy	All	All	All	All	All/All	All week	Deny	No	0	✓	📄	✕

(3) An IPS rule and web application protection rule are added automatically. The scanning result shows that the server has security vulnerabilities and web application risks exist. An IPS rule and web application rule can be created intelligently based on the scanning result. For example, select the third item in the scanning result and click

Avoid Risk to configure web application and vulnerability risk protection.

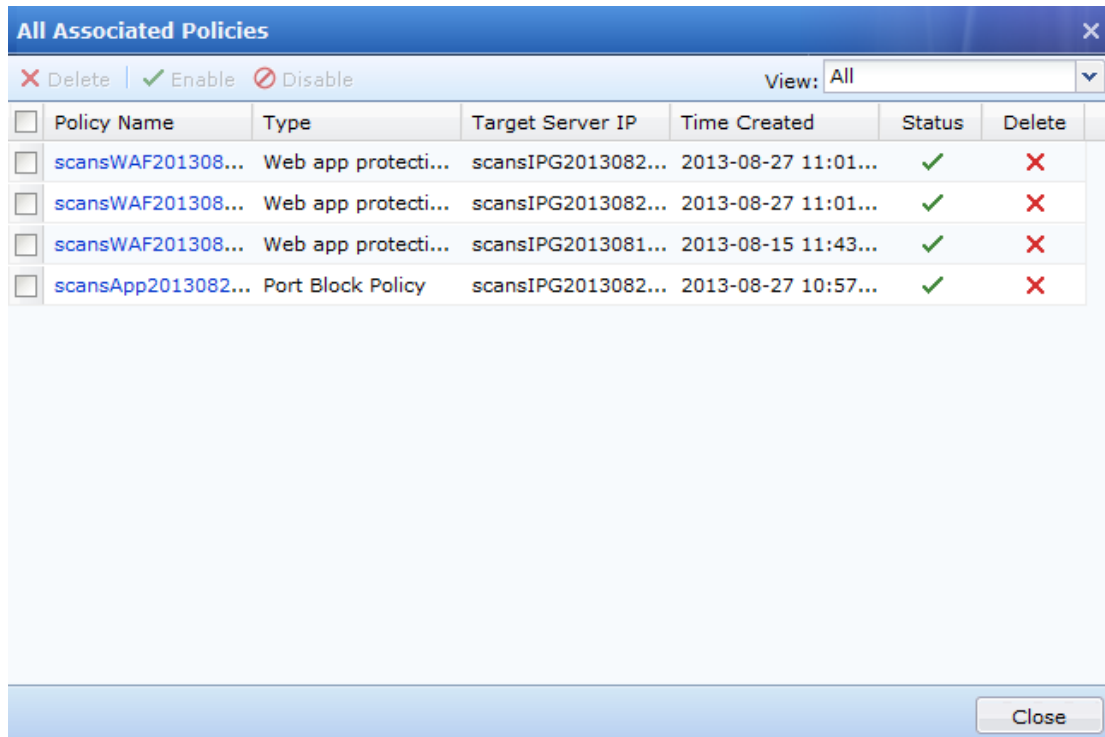
<div> ✓ Avoid Risk Export as PDF All Associated Policies </div> <div> <div>All</div> <div>IP address or port</div> </div>									
Server IP	Port	Applic...	Protocol	Accessibl...	Accessible IP	Threat Le...	Risk		Operation
<input type="checkbox"/>	192.200.17.202	69	tftp	UDP	WAN	0.0.0.0-255.255.255.255	High	Open port risk	
<input type="checkbox"/>	192.200.17.202	21	ftp	TCP	WAN	0.0.0.0-255.255.255.255	High	Weak password risk1	
<input type="checkbox"/>	192.200.17.200	1433	mssql	TCP	WAN	0.0.0.0-255.255.255.255	High	Open port risk	
<input checked="" type="checkbox"/>	192.200.17.22	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	
<input type="checkbox"/>	192.200.17.203	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	
<input type="checkbox"/>	192.200.17.210	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	
<input type="checkbox"/>	192.200.17.202	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Medium	Web vulnerability	
<input type="checkbox"/>	192.200.17.10	53	dns	UDP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.10	445	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.20	53	dns	UDP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	



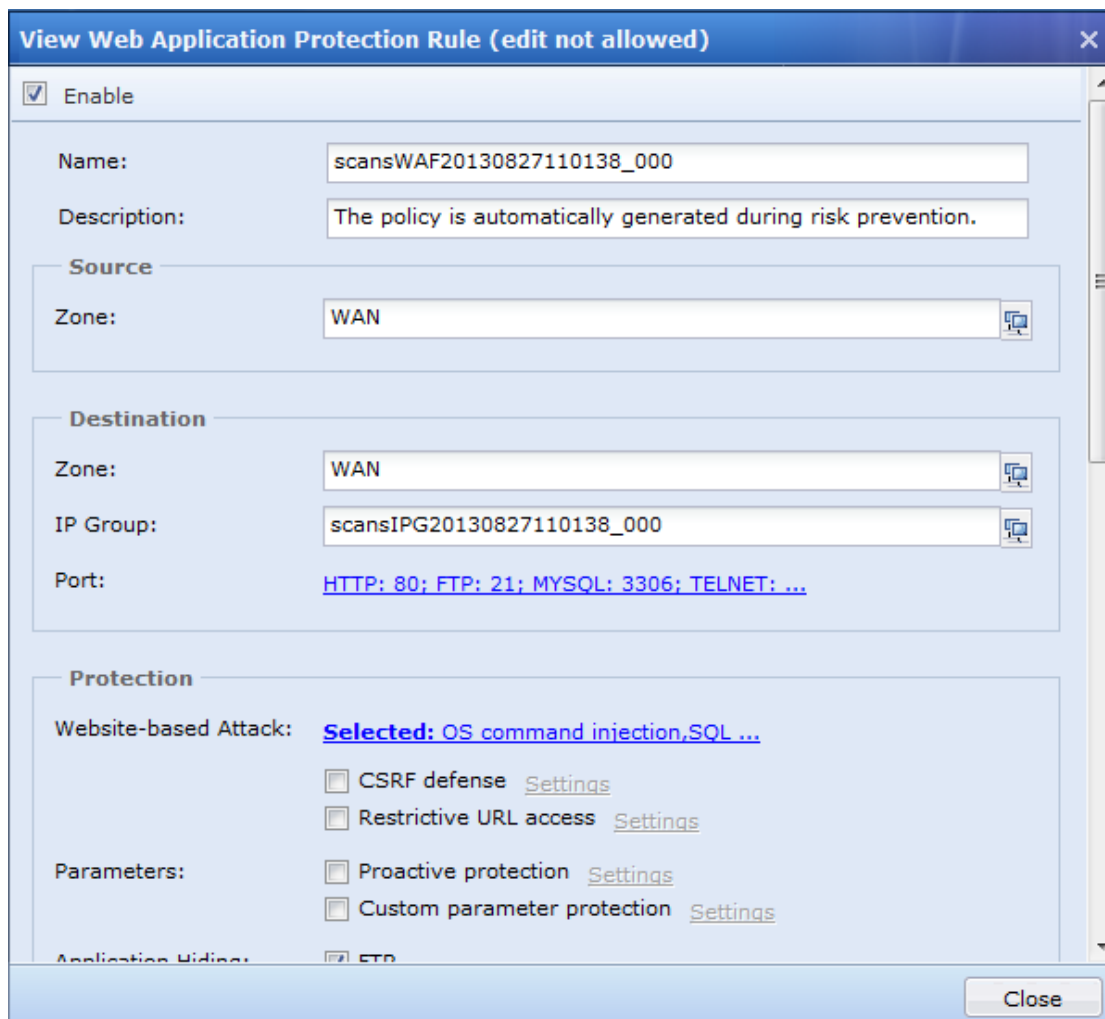
The following information is displayed when protection rules are configured.

<div> ✓ Avoid Risk Export as PDF All Associated Policies </div> <div> <div>All</div> <div>IP address or port</div> </div>									
Server IP	Port	Applic...	Protocol	Accessibl...	Accessible IP	Threat Le...	Risk		Operation
<input checked="" type="checkbox"/>	192.200.17.200	80	http	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.210	443	https	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.232	3389	rdp	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.254	53	dns	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.254	443	https	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.232	445	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.232	139	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.107	139	netbios	TCP	WAN	0.0.0.0-255.255.255.255	Low	Open port risk	
<input type="checkbox"/>	192.200.17.22	3306	mysql	TCP	WAN	0.0.0.0-255.255.255.255	No risk	Port is in protection	
<input checked="" type="checkbox"/>	192.200.17.22	80	http	TCP	WAN	0.0.0.0-255.255.255.255	No risk	Web application is in protection	

Step 7: Click **All Associated Policies** to view the intelligently created protection policies.



Click a policy name to view the policy.



View application control policy (edit not allowed) [X]

☒ Enable

Name: scansApp20130827105718_000

Description: The policy is automatically generated

Source

IP/User: ☒ IP Group
All [icon]

☐ User/Group
Select [icon]

Zone: WAN [icon]

Zone has been selected based on IP group in existing policy. [Yes](#)

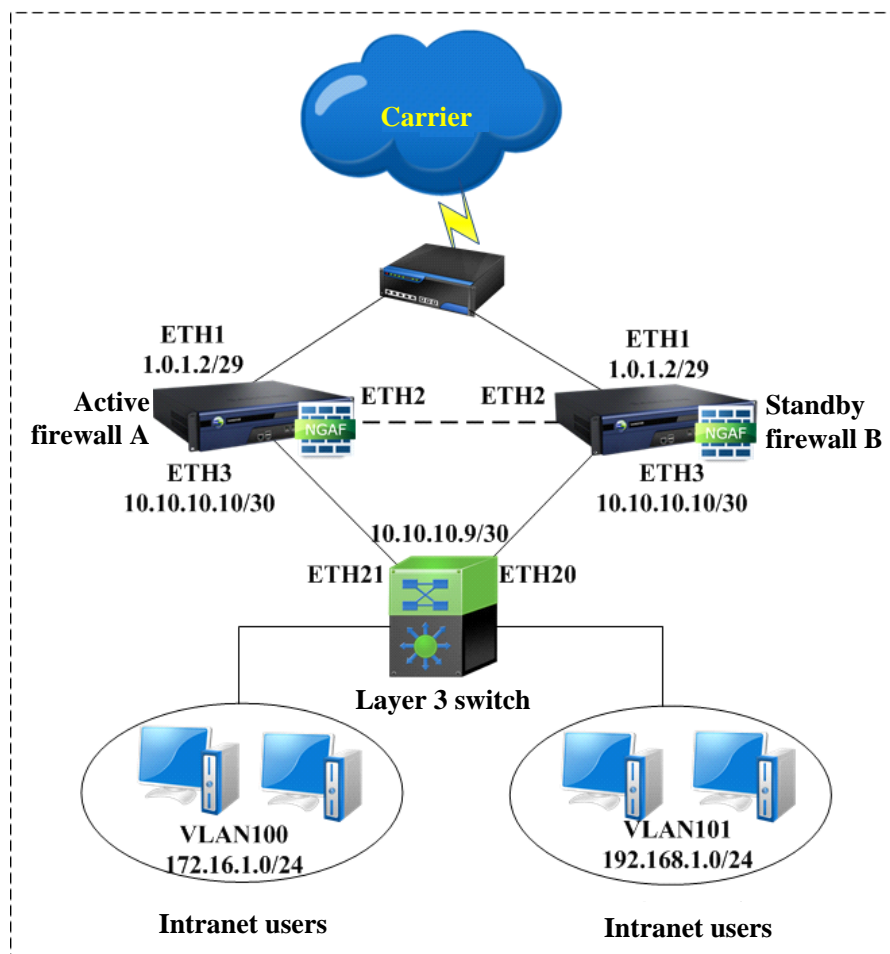
Destination

IP Group: scansIPG20130827105718_000 [icon]

Zone: WAN [icon]

Service/Application

Close



Step 1: Configure firewall A. Choose **Network > Interface > Physical Interface** and configure router interfaces and related information such as IP addresses. For details, see section 3.2.1. Set **ETH1** to **WAN**, **ETH3** to **LAN**, and **ETH2** to **HA**.

Edit Physical Interface

☒ Enable

Name: eth2

Description: HA

Type: Route(layer 3)

Added To Zone: Select zone

Basic Attributes: ☐ WAN attribute ☒ Pingable

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 10.10.9.9/30-HA

Next-Hop IP:

OK Cancel

Interfaces											
Physical Interface											
Name	Interface...	WAN ...	Ping	Type	Zone	IP Assignment	IP Address	Work Mode	MTU	Link State	Status
> eth0	Manage i...	No	Allow	Route(layer 3)	None	Static IP	10.251.251.251/24 192.200.17.22/24	Full-duplex 1... Auto-negotia...	1500	Not detected...	✓
> eth1		No	Allow	Route(layer 3)	WAN	Static IP	1.0.1.2/29	Auto-negotia...	1500	Not detected...	✓
> eth2	HA	No	Allow	Route(layer 3)	DMZ	Static IP	10.10.9.9/30-HA	Auto-negotia...	1500	Not detected...	✓
> eth3		No	Allow	Route(layer 3)	LAN	Static IP	10.10.10.10/24	Auto-negotia...	1500	Not detected...	✓

Step 2: Configure NAT on firewall A and configure firewall A as a proxy to enable intranet users to access the Internet. For details, see section 3.6.2.1.

Step 3: On firewall A, choose **High Availability** > **Basic Settings**, set **Local Device IP** to the IP address of interface ETH2 as the hot standby communication interface, and set **Peer Device IP** to 10.10.9.10.

High Availability

Basic Settings Redundancy Sync Options

Local Device IP: 10.10.9.9/30-HA(eth2)

Peer Device IP: 10.10.9.10

Test

OK

Step 4: On firewall A, choose **High Availability** > **Redundancy** and click **Add**. The **Add VRRP Group** dialog box is displayed. Set **VRID** and **Priority** to 100 and set **Preemption** to **Yes**. Configure interfaces ETH3 and ETH1 as hot standby detection interfaces.

Add VRRP Group

VRID:

100

(1-255)

Priority:

100

(1-255)

Preemption:

☒ Yes
☐ No

Heartbeat Interval:

1

(1-60)s

Member Interfaces:

+

 Add

×

 Delete

<input type="checkbox"/>	No.	Interface	Edit
<input type="checkbox"/>	1	eth1,eth3	

Tracked Interfaces

Available:

eth0
eth4

Selected:

eth1
eth3

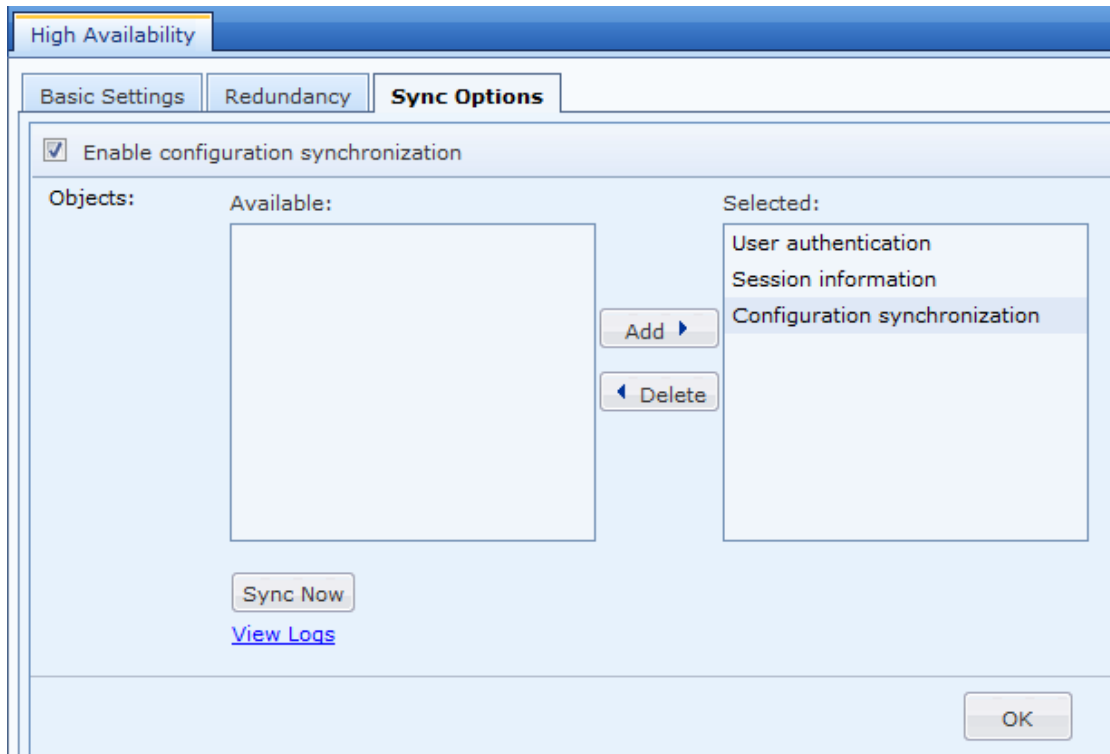
Add

Delete

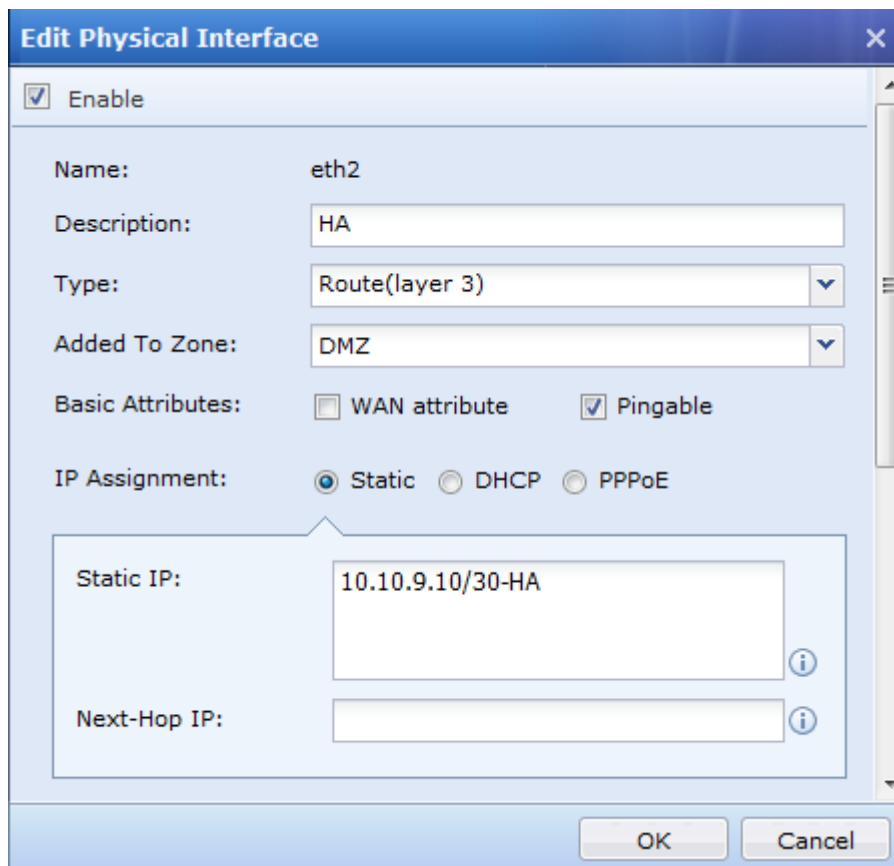
OK

Cancel

Step 5: On firewall A, choose **High Availability > Sync Options**, select **User authentication**, **Session information**, and **Configuration Synchronization**, and click **OK**.



Step 6: Configure firewall B. Only interface ETH2 of firewall B and hot standby data need to be configured. Other settings can be synchronized from firewall A. On firewall B, choose **Network > Interface > Physical Interface** and configure the IP address of interface ETH2.



Step 7: On firewall B, choose **High Availability > Basic Settings**, set **Local Device IP** to the IP address of interface ETH2 and **Peer Device IP** to 10.10.9.9, and click **OK**.

High Availability

Basic Settings | Redundancy | Sync Options

Local Device IP: 10.10.9.10/30-HA(eth2) ⓘ

Peer Device IP: 10.10.9.9 Test ⓘ

OK

Step 8: On firewall B, choose **High Availability** > **Redundancy**, set **VRID** to **100** (which is the same as that of firewall A), set **Priority** to a value smaller than that of firewall A (for example, **90**), set **Preemption** to **No**, set **Heartbeat Interval** to the same value as that of firewall A (a different value will cause data synchronization failure), and select network interfaces.

Add VRRP Group ×

VRID: 100 (1-255)

Priority: 90 (1-255)

Preemption: ☐ Yes ☒ No

Heartbeat Interval: 1 (1-60)s

Member Interfaces: ⓘ

+ Add - Delete	
No.	Interface
1	eth1,eth3

Tracked Interfaces ⓘ

Available:

eth0
eth4

Selected:

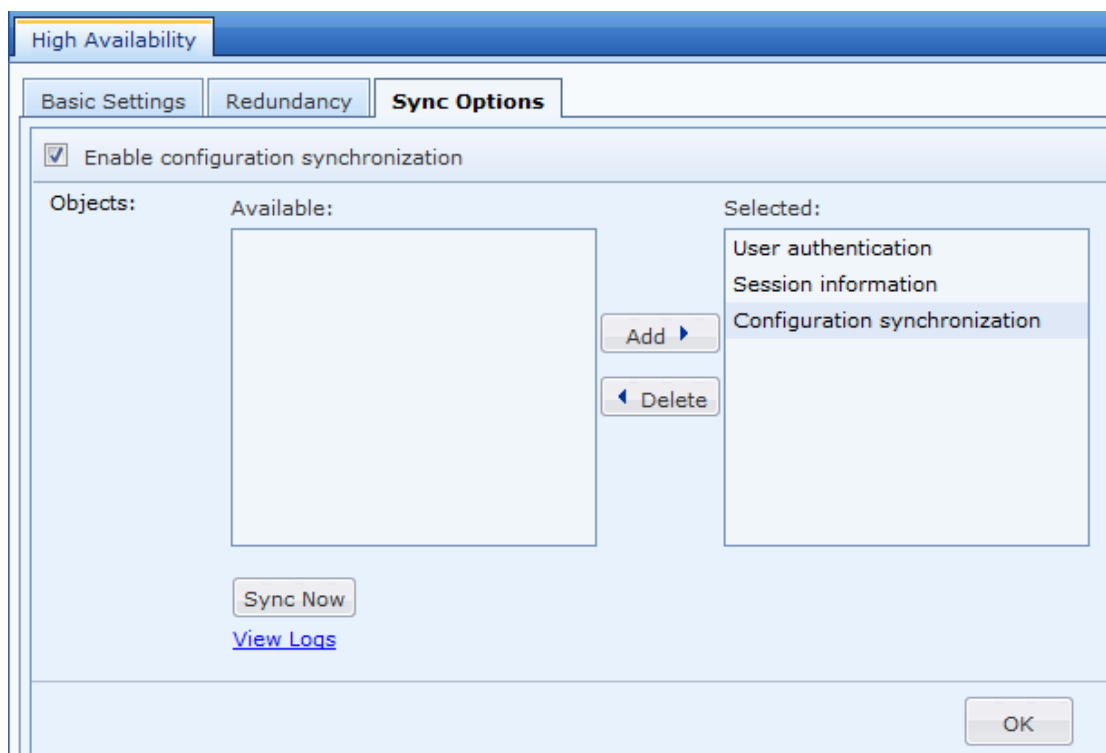
eth1
eth3

Add ▶ ◀ Delete

OK Cancel

Step 9: (Optional) Configure synchronization on firewall B. Choose **High Availability** > **Sync Options** and select synchronized objects. After synchronization is configured, any modification on firewall B is synchronized to

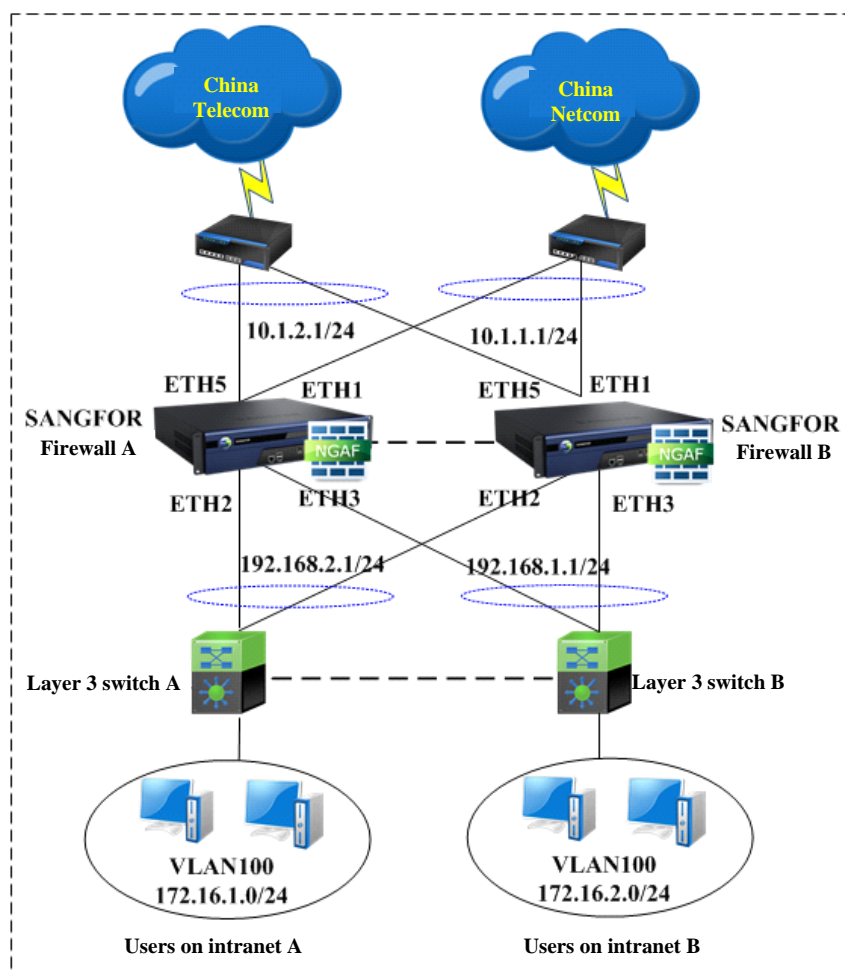
firewall A.



Step 10: Power off firewalls A and B and connect cables. After that, power on firewall A and then firewall B. After being started, firewall B requests configurations from firewall A. Note that firewall B can be powered on only after firewall A is started.

Example 2

The following figure shows a network topology where users on intranet A and intranet B must access the Internet by using lines of China Telecom and China Netcom respectively. Two firewalls (A and B) operate simultaneously to reduce load. Upon failure of a firewall, all data is routed to the other firewall, causing no adverse impact on the network.



Configuration procedure:

1. In the **Add VRRP Group** dialog box, set **VRID** and **Priority** both to **50** for interfaces ETH5 and ETH2 of firewall A and set **VRID** and **Priority** both to **20** for interfaces ETH1 and ETH3 of firewall A.
2. In the **Add VRRP Group** dialog box, set **VRID** to **50** and **Priority** to **40** for interfaces ETH5 and ETH2 of firewall B and set **VRID** to **20** and **Priority** to **30** for interfaces ETH1 and ETH3 of firewall B.
3. When the configuration is completed, users on intranet A access the Internet through interfaces ETH2 and ETH5 of firewall A and users on intranet B access the Internet through interfaces ETH3 and ETH1 of firewall B. Upon failure of an interface, the corresponding interface of the other firewall takes over replacing the faulty interface.
4. Allocate the interfaces of firewalls connected to layer 3 switch A to the same VLAN. The IP address of interface ETH2 is 192.168.2.1/24. The next hop of layer 3 switch A points to 192.168.2.1/24. Configure two routes on firewall A. The next hop to 172.16.1.0/24 is layer 3 switch A and the next hop to 172.16.2.0/24 is layer 3 switch B. The implementation and configuration between layer 3 switch B and firewall B are the same as described above.

Steps:

Step 1: Configure the following data on firewall A: interface IP addresses, NAT, packet reception route, PRB, etc. For details, see preceding sections.

Step 2: On firewall A, choose **High Availability > Basic Settings**, set **Local Device IP** to the IP address of interface ETH4, and set **Peer Device IP** based on requirements. The settings enable firewalls A and B to synchronize configuration and negotiate VRRP.

Step 3: On firewall A, choose **High Availability > Redundancy**, set **VRID** and **Priority** both to **50** for interfaces ETH5 and ETH2; set **VRID** and **Priority** both to **20** for interfaces ETH1 and ETH3, and set **Preemption** to **No**.

Step 4: On firewall A, choose **High Availability > Sync Options** and select all three synchronized objects.

Step 5: Configure the HA interface of firewall B.

Step 2: On firewall B, choose **High Availability > Basic Settings**, set **Local Device IP** to the IP address of interface ETH4, and set **Peer Device IP** based on requirements. The settings enable firewalls A and B to synchronize configuration and negotiate VRRP.

Step 7: On firewall B, choose **High Availability > Redundancy**, set **VRID** to **50** and **Priority** to **40** for interfaces ETH5 and ETH2, and set **Preemption** to **No**; set **VRID** to **20** and **Priority** to **30** for interfaces ETH1 and ETH3, and set **Preemption** to **Yes**.

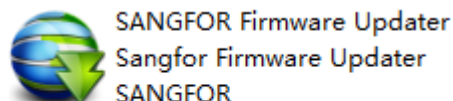
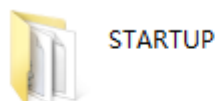
Step 8: On firewall B, choose **High Availability > Sync Options** and select all three synchronized objects.

Step 9: Power off firewalls A and B and connect cables. After that, power on firewall A and then firewall B. After being started, firewall B requests configurations from firewall A. Note that firewall B can be powered on only after firewall A is started.

Appendix: SANGFOR NGAF Upgrade System

The SANGFOR NGAF upgrade system is used to upgrade device kernel versions and back up and restore device configurations. When a device encounters a critical error, the upgrade system can restore the device to factory settings. The upgrade system can enable technical support tools to detect configurations such as the operating status of network interfaces and change the operating mode of network interfaces.

The SANGFOR NGAF upgrade system can be used after the software is decompressed. There are a **STARTUP** folder and a main program.



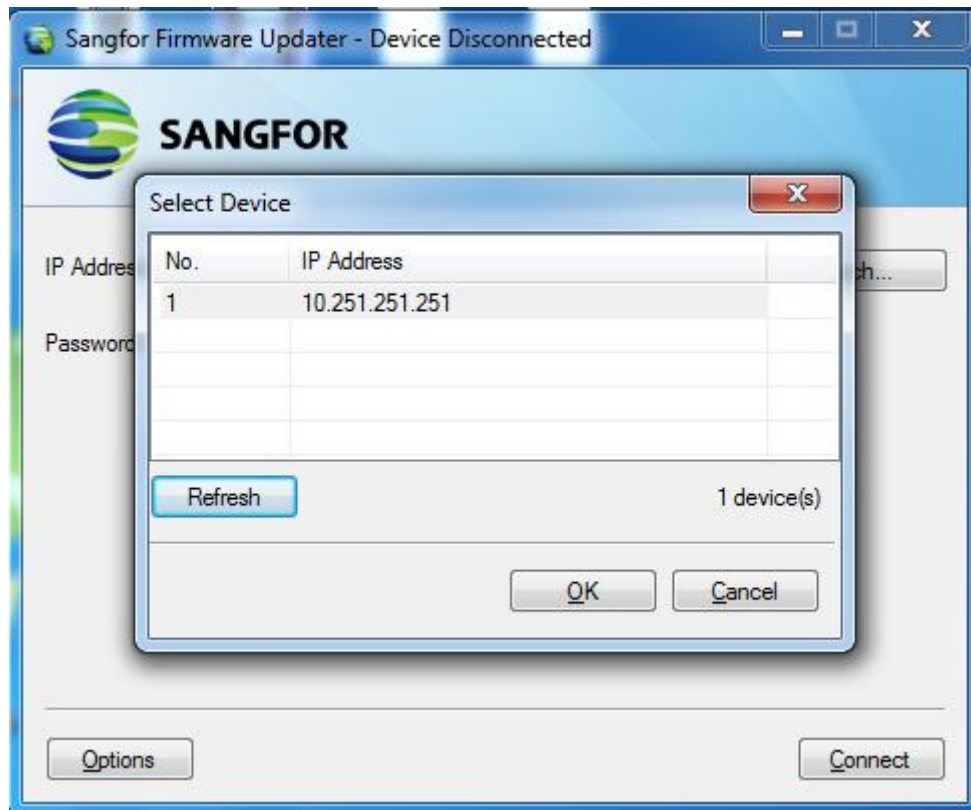
Double-click the icon of the main program. The following page is displayed.



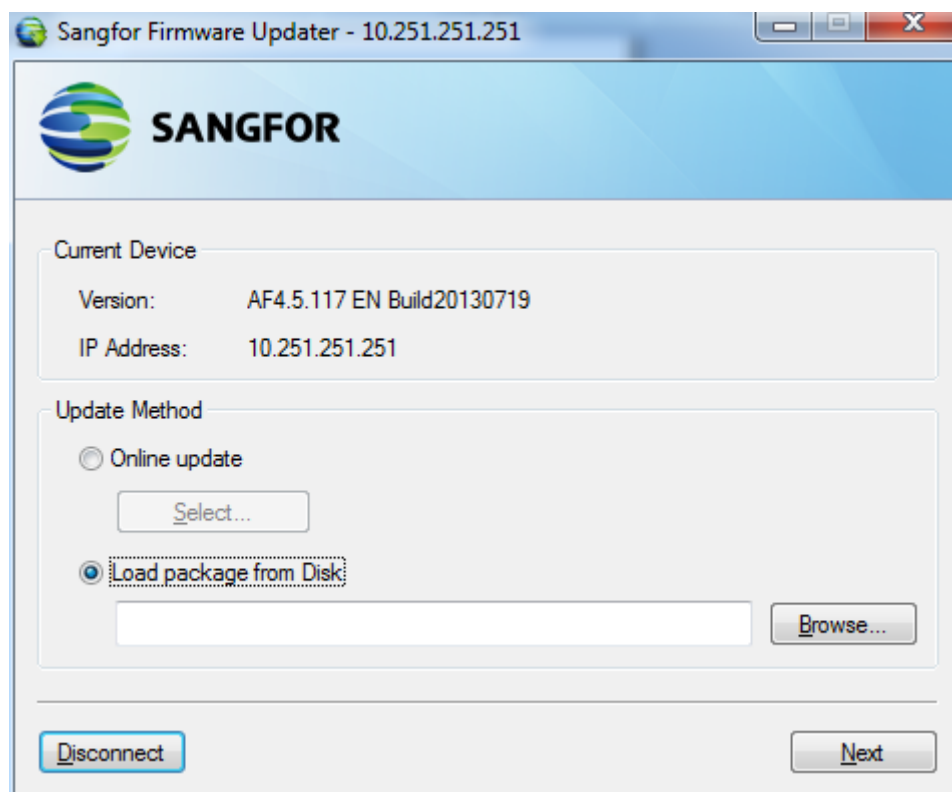
IP Address: specifies the IP address of the connected NGAF, which is in the format of *IP address:port*. When a single IP address is entered, port 51111 is used by default.

Password : specifies the password used to log in to the connected NGAF (the password is related to the device version). The default password is **dlanrecover** or is consistent with the password of the console of the NGAF.

Search: Click it to search for NGAFs on a LAN.



Enter the IP address and admin password of an NGAF and click **Connect** to connect to the NGAF and perform operations such as system upgrade and restoration of default settings.



Current Device: specifies the version information and IP address of the connected NGAF.

Update Method: is used to upgrade the connected SANGFOR NGAF. The options include Online update and Load package from Disk

Online upgrade:

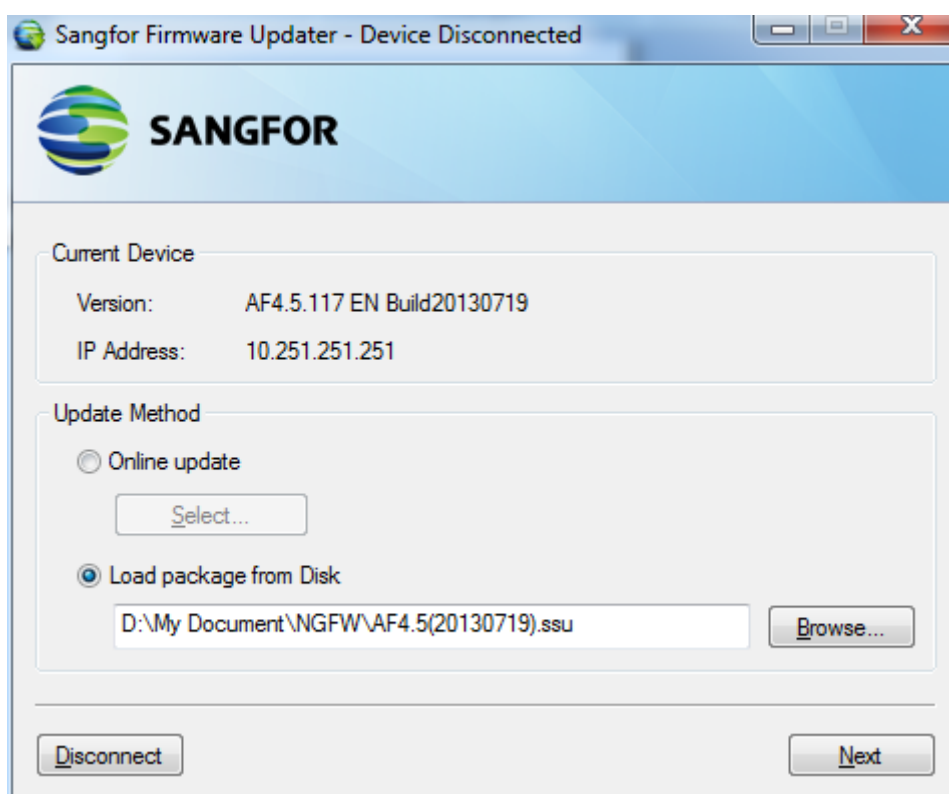
Click Online Update > Select. The SANGFOR NGAF upgrade system lists the versions that the NGAF can be upgraded to. Select a version and click **OK**. The system downloads an upgrade package from a server automatically and starts upgrade.

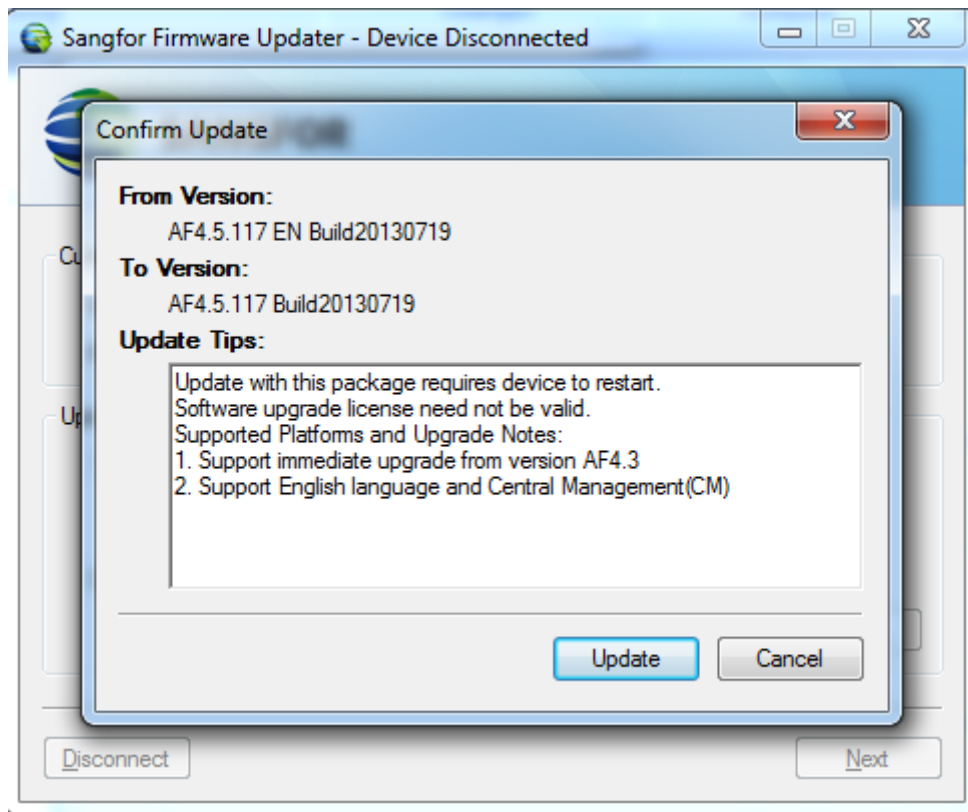


- When the SANGFOR NGAF upgrade system is used for online upgrade, the NGAF must be connected to the Internet normally.
- Some versions of the NGAF do not support online upgrade. For details, contact SANGFOR customer service center.

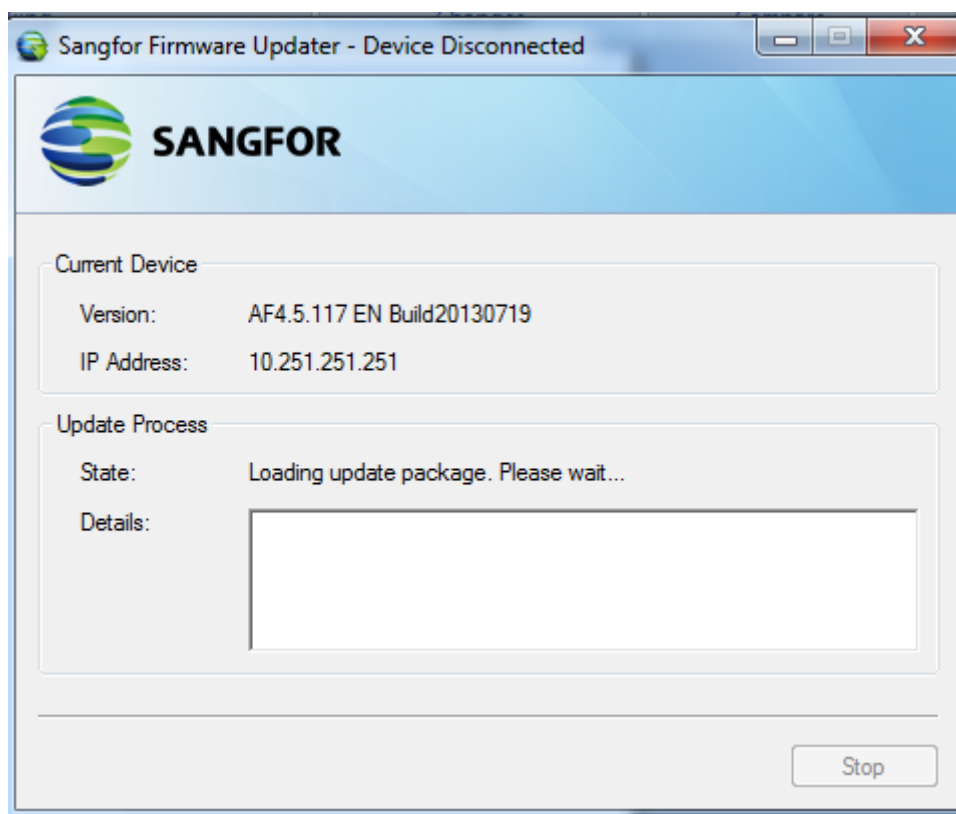
Load Package from Disk:

Click Load Package from Disk > **Browse**, select an upgrade package that has been downloaded to a local disk, and click **Next**. Basic information of the selected upgrade package is displayed. Confirm the information and click Update.





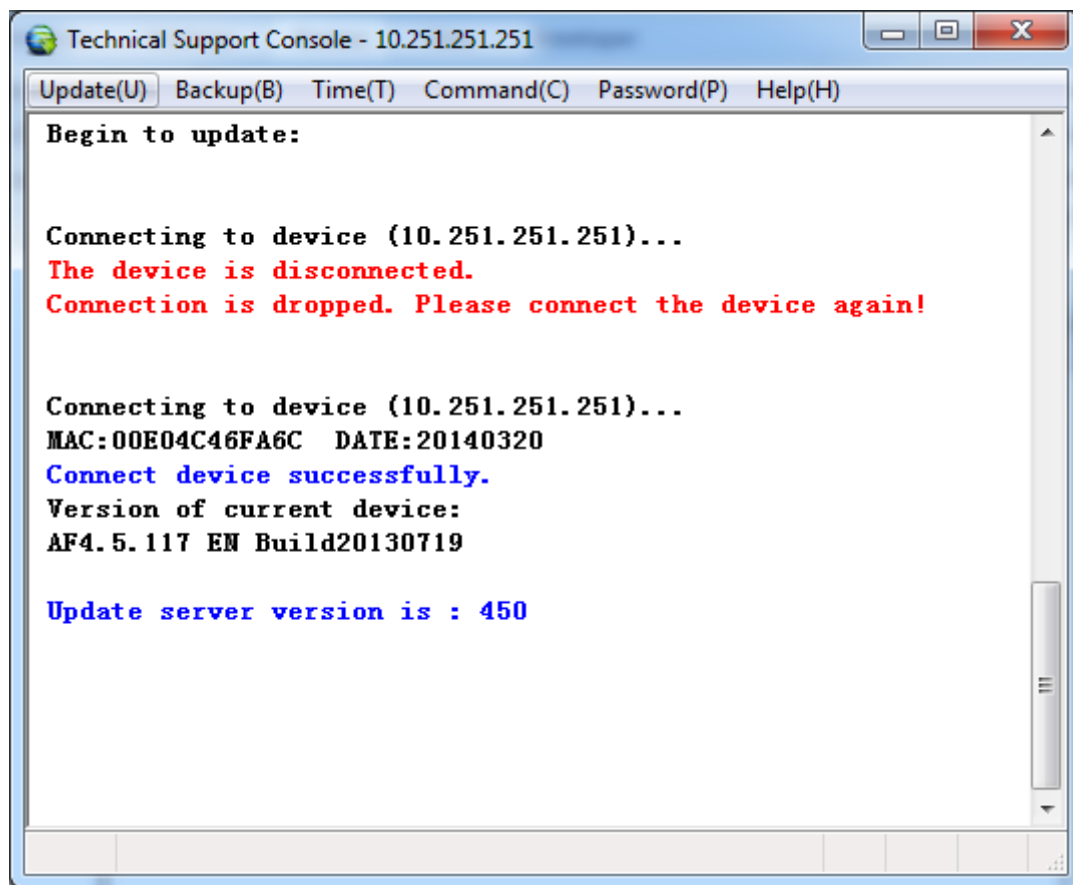
After upgrade, **State** displays update successful in the Update Process area.



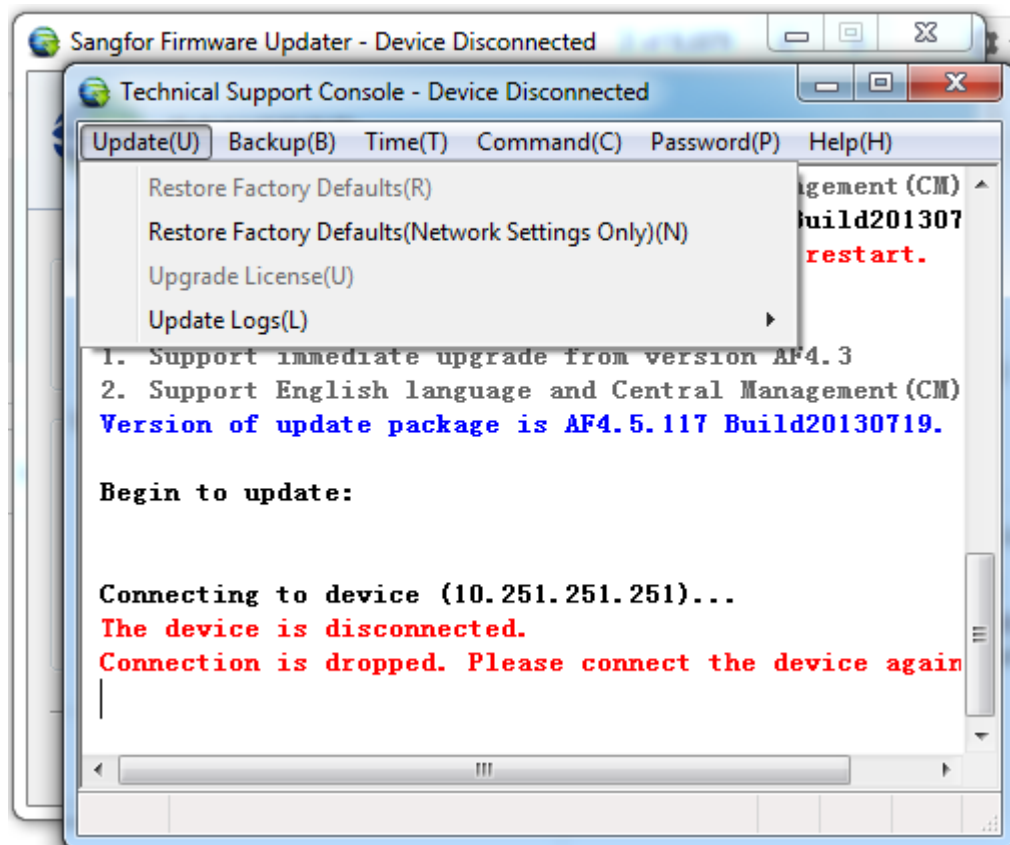
Improper upgrade with cause device damage. Before upgrade, contact SANGFOR customer service department.

Enabling technical support tools:

To enable technical support tools, press **F10** or **Ctrl+Shift+F10** after the SANGFOR NGAF upgrade system is connected to the NGAF. The **Technical Support Tool** dialog box has the **Upgrade**, **Backup**, **Time**, **Command**, **Change Password**, and **Help** menus.



Upgrade: includes the following options: Restore Factory Default, Restore Factory Default (Network Setting Only), Upgrade license, and Update logs.



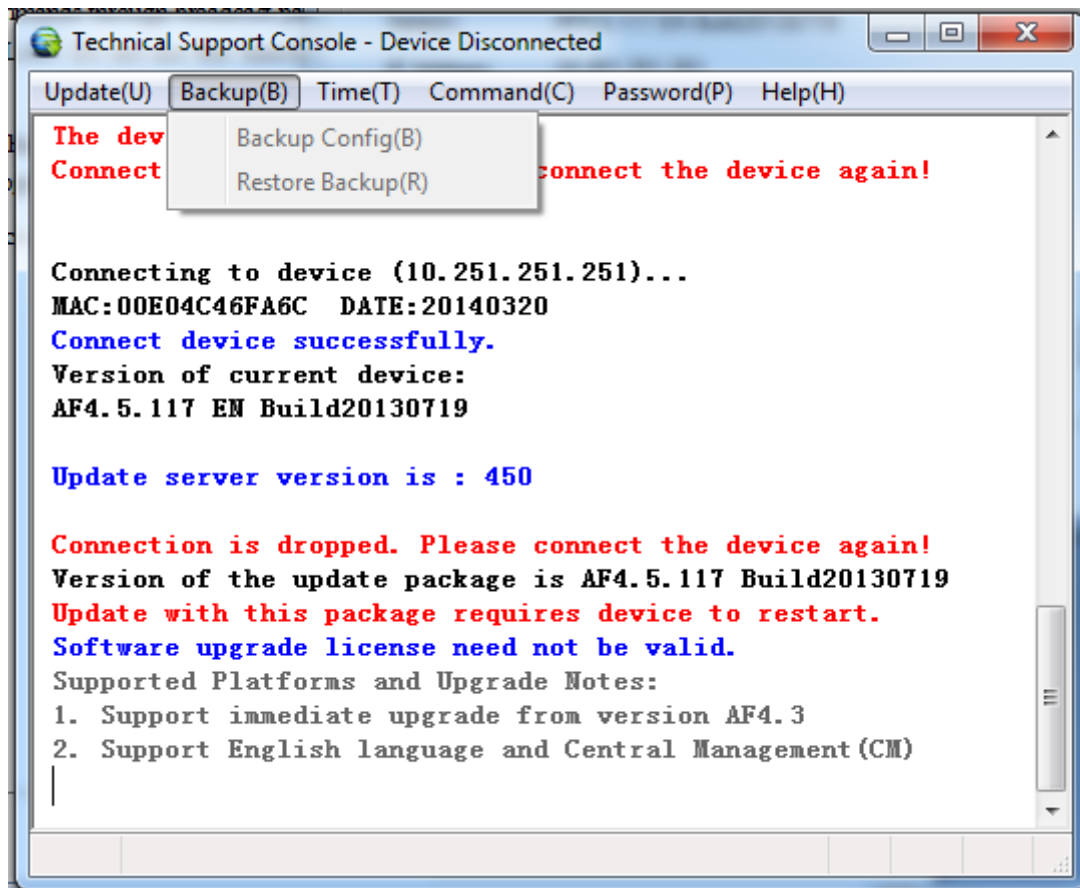
Restore Factory Default: is used to restore SANGFOR hardware to factory settings by loading an upgrade package.

Restore Factory Default (Network Setting Only): (used when the NGAF is not connected) is used to restore the network settings of the NGAF to factory settings by issuing commands through broadcast packets. The operation takes effect for all SANGFOR hardware gateways on a LAN. Do not use this function without authorization.

Upgrade license: is used to check whether the current gateway is within the upgrade service validity period. If the gateway expires, purchase the corresponding license before upgrade.

Update logs: is used to view the upgrade history of the current device or view/clear local historical records of upgrade.

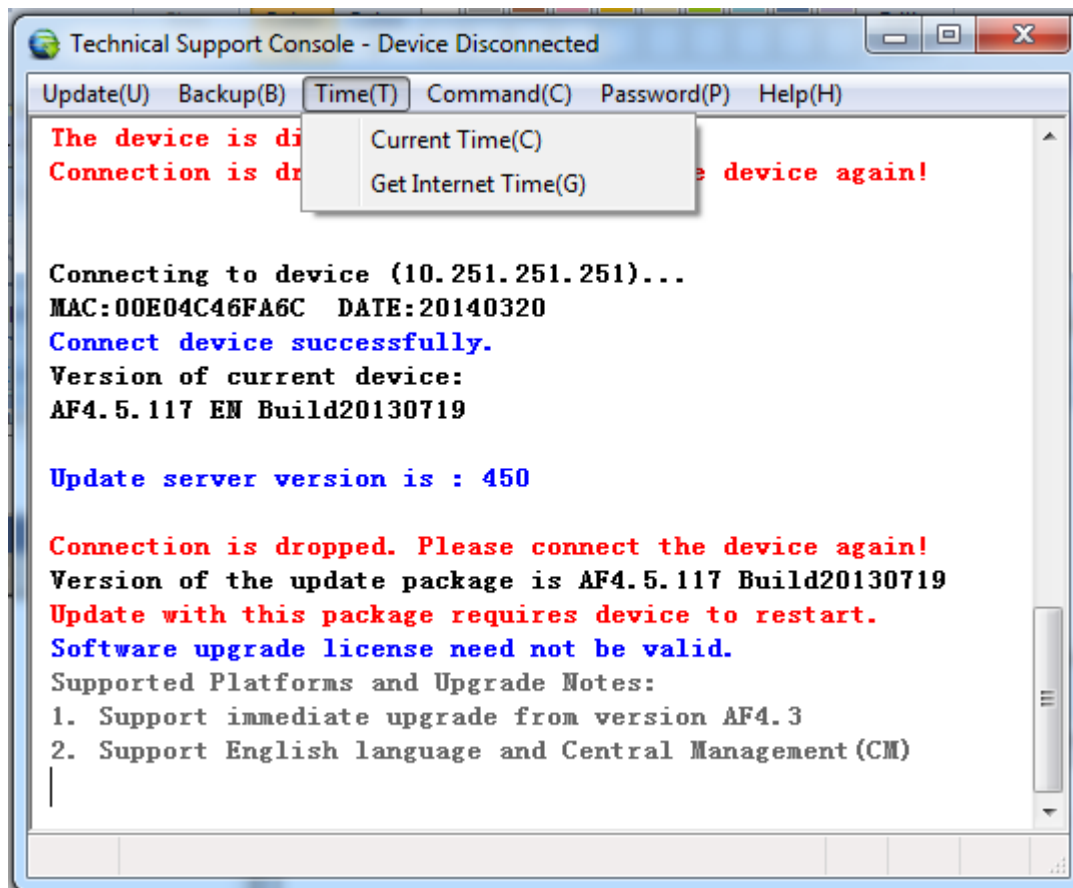
Backup: includes the Backup Config and Restore Backup options.



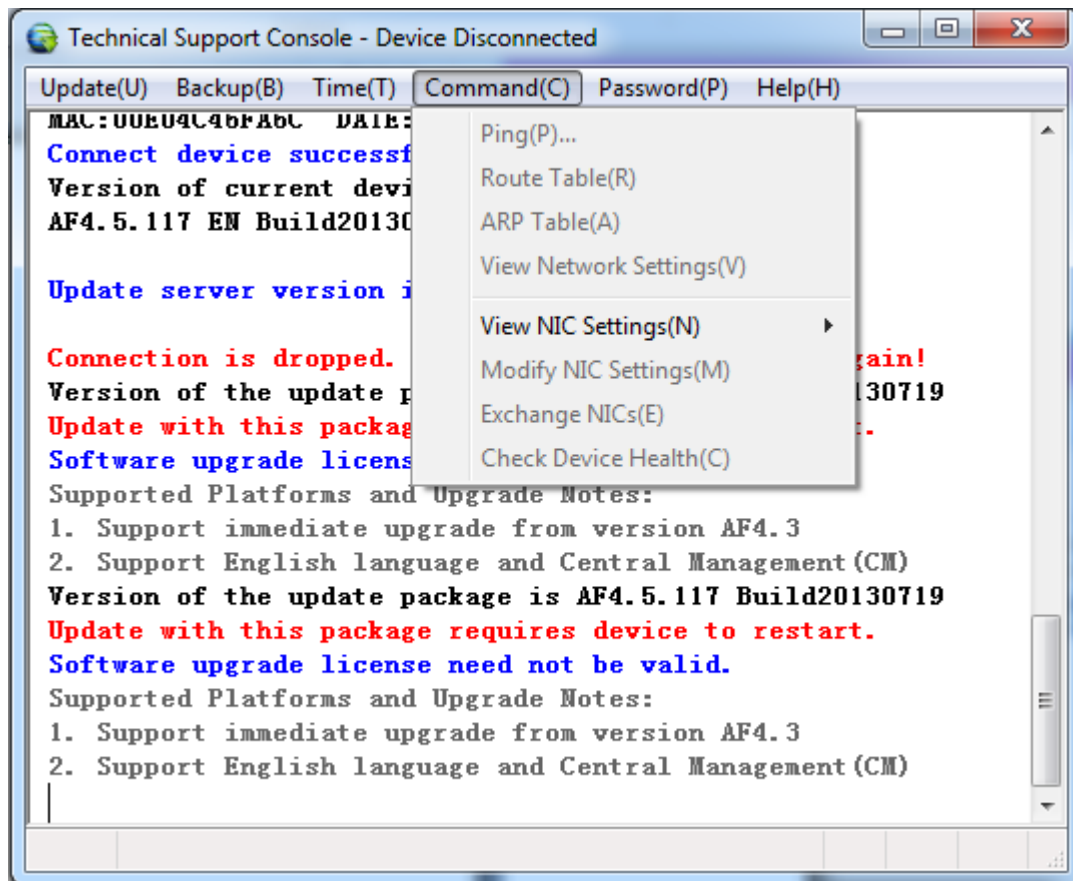
Backup Config: is used to back up device configurations.

Restore Backup: is used to restore backup configurations to the device.

Time: is used to view the current time and synchronize the time of a public network so as to check whether a device upgrade license expires.



Command: include the following options: Route table, ARP table, View Network Setting, View NIC Setting, Modify NIC Setting, Exchange NICs & Check Device Health.



Ping: is used to ping the Internet from the NGAF after login to check whether the NGAF is connected to the Internet.

Route table: is used to view the routing table of the NGAF.

ARP table: is used to view the ARP table of the NGAF.

View Network Setting: is used to view the network settings (such as IP address settings) of the NGAF.

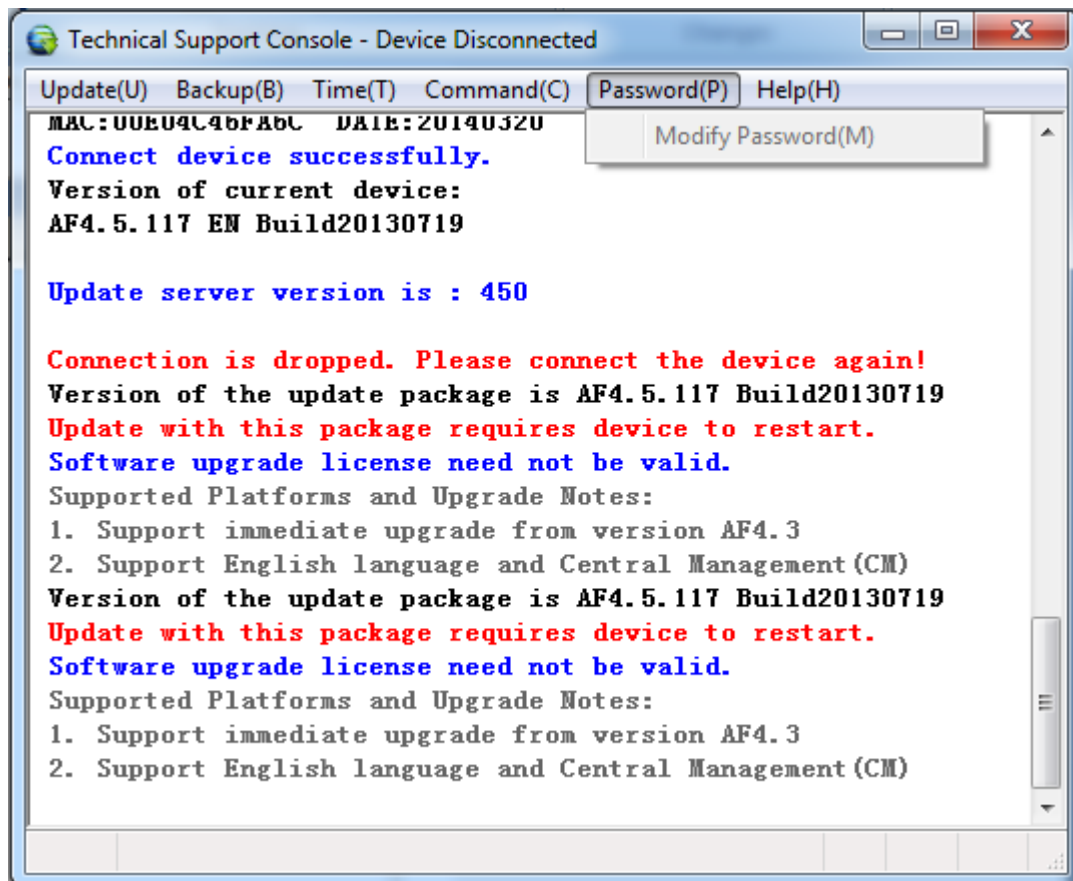
View NIC Setting: is used to view the operating mode of each network adapter of the NGAF.

Modify NIC Setting: is used to view the operating mode of a network adapter.

Exchange NICs: is used to switch the physical positions of network adapters.

Check Device Health: is used to detect the hardware status of the NGAF online or by uploading scripts.

Modify Password: is used to change the password of the SANGFOR upgrade system.



Help: provides the links to the public network homepage and technical support forum and the version information of the current SANGFOR Firmware Updater.

